2000-03

Development of a software evolution process for military systems composed of integrated commercial off the shelf (COTS) components

Hensley, Barry J.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

DEVELOPMENT OF A SOFTWARE EVOLUTION PROCESS FOR MILITARY SYSTEMS COMPOSED OF INTEGRATED COMMERCIAL OFF THE SHELF (COTS) COMPONENTS

by

Barry J. Hensley

March 2000

Thesis Advisor: John Osmundson
Second Reader: Mantak Shing

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	March 2000	Master's Thesis

4. TITLE AND SUBTITLE
Development of a Software Evolution Process for Military Systems Composed of Integrated Commercial off the Shelf Components

5. FUNDING NUMBERS

6. AUTHOR(S)
Hensley, Barry J.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release, distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT

Department of Defense (DoD) acquisition policy requires that military system acquisitions incorporate commercial-off-the-shelf (COTS) components into system architectures. Traditional DoD source code development and evolution methodologies do not effectively support COTS-intensive systems. To fully realize the benefits of COTS technologies and products, the DoD must adopt new ways to sustain system evolution in the face of a dynamic market environment subject to constant change.

This thesis proposes a new software evolution methodology to effectively maintain COTS-intensive military systems. The integrated COTS component evolution (ICCE) model provides evolution processes designed to support the maintainer as a consumer of software instead of a source-code developer. The ICCE model affords proactive risk awareness, market awareness, and user awareness activities. The ICCE model also supports a three-tier test and evaluation process. A case study for the U.S. Navy/Marine Corps Meteorological Mobile Facility Replacement (METMF(R)) program demonstrates the effectiveness of the ICCE risk management process.

14. SUBJECT TERMS	15. NUMBER OF PAGES
COTS, GOTS, Software Evolution, Software Management, Requirements Management, Risk Management, Software Evolution Model	157
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

Approved for public release; distribution is unlimited

DEVELOPMENT OF A SOFTWARE EVOLUTION PROCESS FOR MILITARY SYSTEMS COMPOSED OF INTEGRATED COMMERCIAL OFF THE SHELF (COTS) COMPONENTS

Barry J. Hensley
B.S.E.E., North Carolina State University, 1983

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SOFTWARE ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
March 2000

Author: [redacted]
Barry J. Hensley

Approved by: [redacted]
John Osmundson, Thesis Advisor

[redacted]
Mantak Shing, Second Reader

[redacted]
Luqi, Chairman
Software Engineering Curriculum

[redacted]
Dan Boger, Chairman
Department of Computer Science

ABSTRACT

Department of Defense (DoD) acquisition policy requires that military system acquisitions incorporate commercial-off-the-shelf (COTS) components into system architectures. Traditional DoD source code development and evolution methodologies do not effectively support COTS-intensive systems. To fully realize the benefits of COTS technologies and products, the DoD must adopt new ways to sustain system evolution in the face of a dynamic market environment subject to constant change.

This thesis proposes a new software evolution methodology to effectively maintain COTS-intensive military systems. The integrated COTS component evolution (ICCE) model provides evolution processes designed to support the maintainer as a consumer of software instead of a source-code developer. The ICCE model affords proactive risk awareness, market awareness, and user awareness activities. The ICCE model also supports a three-tier test and evaluation process. A case study for the U.S. Navy/Marine Corps Meteorological Mobile Facility Replacement (METMF(R)) program demonstrates the effectiveness of the ICCE risk management process.

TABLE OF CONTENTS

ACKNOWLEGEMENT

The author wishes to thank

Dr. John Osmundson and Dr. Mantak Shing

for their guidance and support in this endeavor.

I. INTRODUCTION

A. SUMMARY

Department of Defense (DoD) acquisition policy requires that military system acquisitions incorporate commercial-off-the-shelf (COTS) components into system architectures. Traditional DoD source code development and evolution methodologies do not effectively support COTS-intensive systems. To fully realize the benefits of COTS technologies and products, the DoD must adopt new ways to sustain system evolution in the face of a dynamic market environment subject to constant change.

This thesis proposes a new software evolution methodology to effectively maintain COTS-intensive military systems. The integrated COTS component evolution (ICCE) model provides evolution processes designed to support the maintainer as a consumer of software instead of a source-code developer. The ICCE model affords proactive risk awareness, market awareness, and user awareness activities. The ICCE model also supports a three-tier test and evaluation process. A case study for the U.S. Navy/Marine Corps Meteorological Mobile Facility Replacement (METMF(R)) program demonstrates the effectiveness of the ICCE risk management process.

B. PURPOSE

The Department of Defense (DoD) is undergoing a significant change in the way it acquires and maintains software intensive systems. To alleviate software development costs and reduce schedule delays, the DoD is shifting towards the commercial market to fulfill system requirements.

The primary purpose of this thesis is to:

- Develop a new software evolution methodology that supports the DoD maintainer as a consumer of software instead of a source code developer.

The secondary purpose of this thesis is to:

- Develop and demonstrate a risk management process for military systems built around an integrated software component solution.
- Develop a formal qualification test and evaluation process for military systems built around an integrated software component solution.

C. MOTIVATION

> Acquisition managers must understand that choosing a COTS component may be a reasonable solution; however, the decision to use COTS should be the product of analysis, reasoning, and engineering decisions, not the desire to jump on the latest bandwagon. [Ref. 1]

Even though Brooks [Ref. 2] warned that silver bullets do not exist to solve software development and maintenance productivity problems, the DoD is pushing the commercial

market as a silver bullet to reduce military system development costs and to mitigate schedule delays.

A review of software management and engineering literature illustrates some of the following expectations and realities that exist regarding the integration of COTS software components into military systems. Some of the expectations include:

- COTS software components will reduce development costs and overall schedule [Ref. 3].
- COTS software components are less risky [Ref. 4].
- COTS software components can be procured and modified faster and cheaper than developing the component from scratch [Ref. 4].
- COTS software components will satisfy all system requirements [Ref. 4].
- COTS software components are stable and error-free [Ref. 4].
- COTS components do not require testing [Ref. 5].
- COTS components are selected based on extensive evaluation and analysis [Ref. 5].
- Vendors will keep the component current and up to date with technology [Ref. 4].
- Vendors will utilize commercially accepted interface standards.
- Vendors will employ commercially accepted software engineering development practices.
- Vendor literature is accurate, complete and understandable [Ref. 4].
- An open-system architecture solves the COTS component inter-operability problem [Ref. 5].

Some of the realities include:

- COTS software component integration can be expensive [Ref. 4].
- COTS software components require more testing because the integrator does not know how they were built [Ref. 5].
- COTS software components are typically selected based on slick demos, web searches, or by reading trade journals [Ref. 5].
- Selecting the wrong COTS component can be more expensive than fixing problems in custom-built software [Ref. 4].
- COTS software component vendors do not supply all services [Ref. 4].
- Features sell COTS components, not documentation [Ref. 5].
- COTS software components may not meet all the system requirements [Ref. 4].
- COTS software components may not be easy to modify [Ref. 4].
- The system developer will have little control over vendor quality and schedule [Ref. 4].
- The system developer's organization will have to change to accommodate COTS software components [Ref. 4].
- There is no standard definition for open-system and plug-and-play does not always work [Ref. 5].
- COTS software components introduce new tradeoffs, issues, constraints, assumptions, problems, and inadequacies [Ref. 1, 3, 5, 6, 7].

The large-scale integration of COTS software components into military system architectures introduces new engineering, management, and organization challenges:

- The system maintainer no longer controls software component specification.
- The system maintainer no longer controls software component source code.
- The system maintainer no longer controls software component release schedule.
- The system maintainer is no longer able to conduct developmental (white box) test and evaluation.

The purpose of software engineering is to improve the quality of software and software products [Ref. 8]. The primary motivation behind this thesis is to help DoD managers acquire and maintain effective COTS-intensive military systems. Specifically, this paper will attempt to convey the following essential points:

- DoD managers and engineers must have a clear understanding of the applicable risks and benefits associated with COTS-intensive system acquisitions.
- DoD managers and engineers must adopt new processes and activities to sustain effective COTS-intensive systems.

D. ORGANIZATION

This thesis is organized into the following sections:

- Section II identifies acquisition source documents and policy statements affecting the DoD's push toward COTS integration into military systems.
- Section III provides a brief overview of traditional source code-based development and evolution activities.
- Section IV presents the integrated COTS component evolution (ICCE) model along with a brief overview of the major ICCE activities and processes.
- Section V presents the ICCE risk management process for COTS-intensive systems.
- Section VI presents a case study that demonstrates the effectiveness of the ICCE risk management process.
- Section VII presents the ICCE test and evaluation process for COTS-intensive systems.
- Section VIII provides thesis conclusions and recommendations.

II. BACKGROUND

A. DOD ACQUISITION POLICY SHIFT

> Organizations that acquire software-intensive systems have undergone a remarkable change in emphasis toward use of existing commercial products. This shift is especially noticeable in U.S. Government procurements, particularly those of the Department of Defense (DoD). [Ref. 1]

The primary policy documents for DoD system acquisition include the Federal Acquisition Regulation (FAR), the Defense Federal Acquisition Regulation Supplement (DFARS), DoD Directive 5000.1, and DoD Regulation 5000.2-R.

1. Federal Acquisition Regulation (FAR)

The FAR codifies uniform policies for acquisition of supplies and services by executive agencies. DoD implementation and supplementation of the FAR is issued in the DFARS under authorization of the Secretary of Defense. The FAR provides the following COTS-related policy statements [Ref. 9]:

Part 7 Acquisition Planning; Subpart 7.1 Acquisition Plans; Subpart 7.102 Policy:

> (a) Agencies shall perform acquisition planning and conduct market research (see Part 10) for all acquisitions in order to promote and provide for (1) Acquisition of commercial items or, to the extent that commercial items suitable to meet the agency's needs are not available, nondevelopmental items, to the maximum extent practicable (10 U.S.C. 2377 and 41 U.S.C. 251, et seq.).

Part 10 Market Research; Subpart 10.001 Policy:

> (a) Agencies shall ... (3) Use the results of market research to (i) determine if sources capable of satisfying the agency's requirements exist; (ii) Determine if commercial items or, to the extent commercial items suitable to meet agency's needs are not available, nondevelopmental items are available that (A) Meet the agency's requirements; (B) Could be modified to meet the agency's requirements; or (C) Could meet the agency's requirements if those requirements were modified to a reasonable extent; (iii) Determine the extent to which commercial items or nondevelopmental items could be incorporated at the component level.

Part 12 Acquisition of Commercial Items; Subpart 12.1 Acquisition of Commercial Items - General; Subpart 12.101 Policy:

> Agencies shall (a) Conduct market research to determine whether commercial items or nondevelopmental items are available that could meet the agency's requirements; (b) Acquire commercial items or nondevelopmental items when they are available to meet the needs of the agency; and (c) Require prime contractors and subcontractors at all tiers to incorporate, to the maximum extent practicable, commercial items or nondevelopmental items as components of items supplied to the agency.

2. DoD Directive 5000.1, March 1996

DoD Directive 5000.1 provides mandatory acquisition policies and procedures for all defense acquisition programs. The current release of DoD Directive 5000.1 includes change 1 (administrative re-issuance), May 21, 1999 and provides the following COTS-related policy statement [Ref. 10]:

Section 4 Policy; 4.2 Acquiring Quality Products; 4.2.2 Hierarchy of Material Alternatives:

> In response to operational requirements, priority consideration shall always be given to the most cost-effective solution over the system's life-cycle. Generally, use or modification of systems or equipment that the Department already owns is more cost-effective than acquiring new materiel. If existing U.S. military systems or other on-hand materiel cannot be economically used or modified to meet the operational requirement, an acquisition program may be justified and acquisition decision-makers shall observe the following hierarchy of alternatives: (1) the procurement (including modification) of commercially available systems or equipment, the additional production (including modification) of already-developed U.S. military systems or equipment, or Allied systems or equipment; (2) cooperative development program with one or more Allied nations; (3) new joint Service development program; and (4) a new Service-unique development program. Important in this evaluation process for new or modified systems are considerations for compatibility, interoperability, and integration with existing and future components or systems.

3. DoD Regulation 5000.2-R, March 1996

DoD Regulation 5000.2-R implements DoD Directive 5000.1 and provides policies and procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs. The current version of DoD Regulation 5000.2-R includes the following modifications: change 1, December 13, 1996; change 2, October 6, 1997; and, change 3, March 23, 1998. DoD Regulation 5000.2-R provides the following COTS-related policies and procedures [Ref. 11]:

Part 2 Program Definition; Section 2.3 Requirements Evolution:

> In the process of refining requirements, key concepts that shall be adhered to include: 1. keeping all reasonable options open and facilitating trade-offs throughout the acquisition process; 2. avoiding early commitments to system-specific solutions, including those that inhibit future insertion of new technology and commercial or non-developmental items; 3. defining requirements in broad operational capability terms; and 4. using minimum acceptable operational performance (thresholds) to establish operational test criteria.

Part 2 Program Definition; Section 2.3 Requirements Evolution; 2.3.1 Evaluation of Requirements Based on Commercial Market Potential:

> Researching the potential of the commercial marketplace to meet system performance requirements is an essential element of building a sound set of requirements. In developing system performance requirements, DoD Components shall evaluate how the desired performance requirements could reasonably be modified to facilitate the use of potential commercial or non-developmental items, components, specifications, open standards, processes, technology, and sources (10 USC §2377; CCA). The results of the evaluation shall be included as part of the initial ORD.

Part 3 Program Structure; Section 3.3 Acquisition Strategy; 3.3.1 Open Systems:

> PMs shall specify open systems objectives and document their approach for measuring the level of openness of systems, subsystems, and components to be acquired, and devise an open systems strategy to achieve these requirements. An open systems strategy focuses on fielding superior warfighting capability more quickly and more affordably by using multiple suppliers and commercially supported practices, products, specifications, and standards, which are selected based on performance, cost, industry acceptance, long term availability and supportability, and upgrade potential.

Part 3 Program Structure; Section 3.3 Acquisition Strategy; 3.3.2 Sources:

In developing and updating the acquisition strategy, the PM shall consider all prospective sources of supplies and/or services that can meet the need, both domestic and foreign. Commercial and non-developmental items shall be considered as the primary source of supply (10 USC §2377; CCA).

Part 3 Program Structure; Section 3.3 Acquisition Strategy; 3.3.2 Sources; 3.3.2.1 Commercial and Non-Developmental Items:

Market research and analysis shall be conducted to determine the availability and suitability of existing commercial and non-developmental items prior to the commencement of a development effort, during the development effort, and prior to the preparation of any product description. The PM shall define requirements (including hardware, software, standards, data, and automatic test systems) in terms that enable and encourage offerors to supply commercial and non-developmental items and provide offerors of commercial and non-developmental items an opportunity to compete in any procurement to fill such requirements. The PM shall require prime contractors and subcontractors at all levels to incorporate commercial and non-developmental items as components of items supplied and shall modify requirements to the maximum extent practicable, to ensure that the requirements can be met by commercial and non-developmental items (10 USC §2377).

Preference shall be given to the use of commercial items first and non-developmental items second.

Part 3 Program Structure; Section 3.3 Acquisition Strategy; 3.3.2 Sources; 3.3.2.3 Industrial Capability:

Program needs shall be met through reliance on a national technology and industrial base sustained primarily by commercial demand. Programs shall minimize the need for new defense-unique industrial capabilities.

Part 3 Program Structure; Section 3.3 Acquisition Strategy; 3.3.5 Contract Approach; 3.3.5.1 Competition:

The Head of each DoD Component with acquisition responsibilities shall designate a competition advocate for the Component and in each procurement activity as a resource to help the Component Head to achieve a competitive environment and promote the acquisition of commercial items (41 USC §418 and 10 USC §2318).

The advocate for competition for each procuring activity shall be responsible for promoting full and open competition, promoting the acquisition of commercial items, and challenging barriers to such acquisition, including such barriers as unnecessarily restrictive statements of need, unnecessarily detailed specifications, and unnecessarily burdensome contract clauses.

Part 3 Program Structure; Section 3.3 Acquisition Strategy; 3.3.5 Contract Approach; 3.3.5.2 Best Practices:

> PMs shall avoid imposing government-unique requirements that significantly increase industry compliance costs. Examples of practices designed to accomplish this direction include: IPPD performance-based specifications, management goals, reporting and incentives; open systems approach (that emphasizes commercially supported practices, products, specifications, and standards); replacement of government-unique management and manufacturing systems with common, facility-wide systems; realistic cost estimates and cost objectives, adequate competition among viable offerors; best value evaluation and award criteria; use of past performance in source selection, results of software capability evaluations; government-industry partnerships; and the use of pilot programs to explore innovative practices.

4. Other References:

Oberndorf and Carney [Ref. 12] examine several additional documents that contain official guidance regarding the use of COTS components in government systems. They include:

- Clinger-Cohen Act, August 1996.
- OMB Memorandum, October 96 (Raines Rules).
- DoD Joint Technical Architecture, August 1996.
- DII COE, April 1997.

The Clinger-Cohen Act applies to all federal government agencies. It addresses information technology and supersedes the 1994 Federal Acquisition Streamlining Act (FASA) and the 1995 Federal Acquisition Reform Act (FARA).

The Raines Rules memorandum applies to all federal government agencies. It addresses information technology and provides additional guidance regarding the Clinger-Cohen Act.

The DoD Joint Technical Architecture (JTA) applies to DoD agencies. It addresses information technology and command, control, communication, computer, and intelligence (C4I) programs. The DoD JTA replaces the Technical Architecture Framework for Information Management (TAFIM).

The Defense Information Infrastructure Common Operating Environment (DII COE) applies to DoD agencies. It addresses information technology.

B. OFF-THE-SHELF (OTS) COMPONENT TERMINOLOGY

This section provides definitions for the following OTS component variations:

- Commercial-Off-the-Shelf (COTS).
- Government-Off-the-Shelf (GOTS).
- Modified-Off-the-Shelf (MOTS).
- Non-Developmental Items (NDI).

Unless specified otherwise, this paper uses the generic term COTS in reference to COTS, GOTS, and NDI components.

1. Commercial OTS (COTS) Software Components

DOD Regulation 5000.2-R defines a commercial item as:

> any item, other than real property, that is of a type customarily used for nongovernmental purposes and that: (1) has been sold, leased, or licensed to the general public; or, (2) has been offered for sale, lease, or license to the general public; or any item that evolved through advances in technology or performance and that is not yet available in the commercial marketplace, but will be available in the commercial marketplace in time to satisfy the delivery requirements under a Government solicitation. Also included in the definition are services in support of a commercial item, or a type offered and sold competitively in substantial quantities in the commercial marketplace based on established catalog or market prices for specific tasks performed under standard commercial terms and conditions; this does not include services that are sold based on hourly rates without an established catalog or market price for a specific service performed (FAR 2.101).

DoD Regulation 5000.2-R defines open system-based commercial items as:

> commercial items that use open standards as their primary interface standards and are selected based on the criteria specified under the section called "Open Systems" (see 3.3.1).

2. Modified OTS (MOTS) Software Component

DoD Regulation 5000.2-R defines a modified commercial item as:

> any item with modifications of a type customarily available in the commercial marketplace or minor modifications of a type not customarily available in the commercial marketplace made to meet Federal Government requirements. Such modifications are considered minor if the change does not significantly alter the nongovernmental function or essential physical characteristics of an item or component, change the purpose of the process. Factors to be considered in determining whether a modification is minor include the value and size of the modification and the comparative value and size of the final product. Dollar values and percentages may be used as guideposts, but are not conclusive evidence that a modification is minor.

3. Government OTS (GOTS) Software Component

GOTS is the Government equivalent of COTS. This paper considers GOTS as any software product that is developed, produced, and controlled by a Government agency.

4. Non-Developmental Item (NDI)

DoD Regulation 5000.2-R defines a non-developmental item as:

> (1) any previously developed item of supply used exclusively for governmental purposes by a Federal Agency, a State or local government, or a foreign government with which the United States has a mutual defense cooperation agreement; (2) any item described in (1) that requires only minor modification or modifications of a type customarily available in the commercial marketplace in order to meet the requirements of the procuring department or agency; or (3) any item of supply being produced that does not meet the requirements described in (1) or (2) solely because the item is not yet in use (FAR 2.101).

DoD Regulation 5000.2-R defines open system-based non-developmental items as:

> non-developmental items that use open standards as their primary interface standards and are selected based on the criteria specified under the section called "Open Systems" (see 3.3.1).

C. COTS SOFTWARE COMPONENT SOLUTION PROFILES

Brownsword, Carney, and Oberndorf [Ref. 7] and Wallnau [Ref. 13] discuss two types of COTS software component solutions. They include the following system profiles:

- Single COTS Component Solution.
- Integrated COTS Component Solution.

1. Single COTS Component Solution

The single COTS software component solution refers to a system built around a single, stand-alone COTS software component. The single component system reflects the following characteristics:

- The system relies on a single technology.
- The system is composed of a single, substantial component.
- The system tends to support a single function (e.g., financial tracking).
- The system developer interfaces with a single vendor.
- The component vendor is the component maintainer.

- The component requires no integration with other components.
- The engineering focus is on component tailoring and configuration.
- The system requires little or no custom-built code.

2. Integrated COTS Component Solution

The integrated COTS software component solution refers to a system built around multiple COTS software components. The system developer acquires and integrates individual COTS software components into a complete system. The multiple component system reflects the following characteristics:

- The system relies on multiple technologies.
- The system is composed of a collection of components.
- The system supports a wide range of functions (e.g., data acquisition/manipulation, communications, database, and product dissemination).
- The system developer interfaces with multiple vendors.
- The system developer is the maintainer.
- The engineering focus is on component integration.
- The system may require limited custom-built code to support component integration (e.g., wrappers, glue code).

III. TRADITIONAL SOFTWARE DEVELOPMENT AND EVOLUTION

A. TRADITIONAL SOFTWARE DEVELOPMENT

> Currently, documented software development lifecycle processes provide little practical guidance to developers to achieve the advantages of COTS software or to assist in the selection of specific products from the myriad available. [Ref. 14]
>
> The currently available inventory of documented process methods has a limitation: most assume the system being built will be coded largely from scratch. As a result, the processes do not address many of the challenges associated with building systems that contain large amounts of commercial-off-the-shelf (COTS) software. [Ref. 3]

This section provides a brief overview of the traditional software development process as outlined by various DoD and commercial software development standards. The primary goals of early DoD software development standards were to provide [Ref. 15]:

- A structured, uniform approach to software development and acquisition.
- The means to establish, evaluate, and maintain quality in software and associated documentation.
- A mechanism for Government insight into the software development, testing, and evaluation activities.

DoD software development standards typically prescribed activities formulated to produce source code. These activities were meant to be independent of development methodology: software activities could be applied

sequentially in support of a classical waterfall development effort or incrementally in support of an evolutionary development effort.

Figure 1 represents a traditional software development process [Ref. 16]. The process provides the following source code development activities:

- Requirements analysis.
- Architecture & detailed design.
- Code & unit (white-box) test.
- Integration test.
- Formal qualification test.

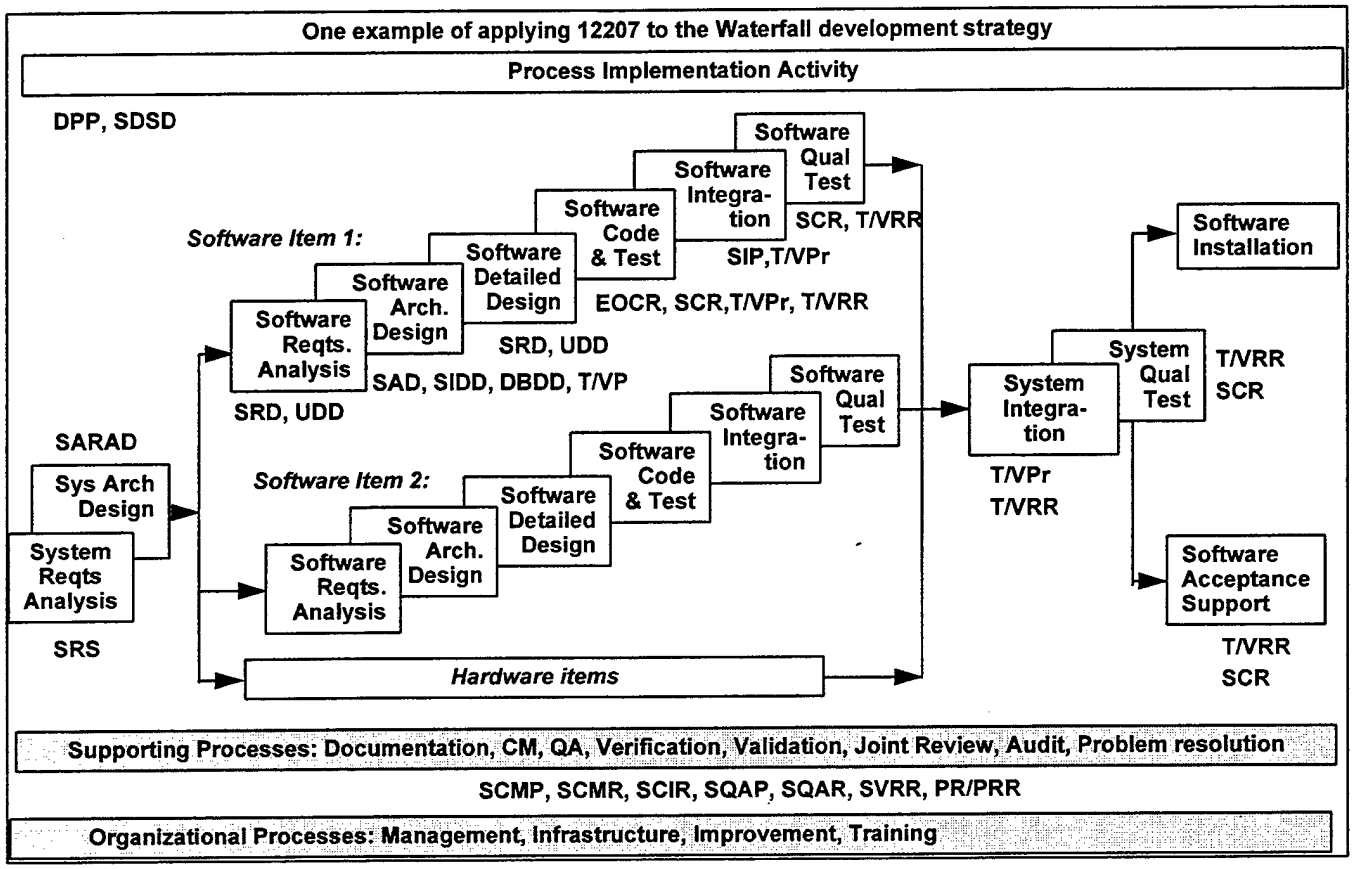

Figure 1. Traditional Software Development Process. From Ref. [16].

1. Traditional Requirements Analysis Activities

Traditional requirements analysis activities include system requirements analysis, hardware component requirements analysis, and software component requirements analysis.

System developers translate general, high-level operational requirements and mission need statements into

very specific, well-defined system requirements. These requirements are documented in a System Specification.

System requirements are further decomposed into detailed sub-requirements that are allocated to mutually exclusive hardware and software configuration items. A Software Requirements Specification captures the software sub-requirements allocated to a particular software configuration item.

The system specification constitutes the Functional Baseline. The aggregate hardware and software component specifications constitute the Allocated Baseline. The Functional and Allocated Baselines are placed under Government configuration management. All requirements changes to these baseline documents are formally controlled and assessed for program cost, schedule, and operational impact. The Functional and Allocated Baselines provide the foundation for all subsequent design, development and qualification activities.

2. Traditional Design and Development Activities

Traditional design and development activities include preliminary (architecture) design, detailed design, coding, developmental (white-box) testing, and integration testing.

Software engineers design components that satisfy the component requirements specified in the Allocated Baseline.

A system component design document captures a component's design information.

Software programmers write code and conduct developmental (white box) testing to satisfy the design requirements identified in a component design document.

Component design documents, source code, and associated development data (e.g., design decision rationale, raw data, developmental test plans, test cases, test procedures, test results, etc.) constitute the system's developmental configuration. The developmental configuration is typically placed under the developer's configuration control.

3. Traditional Formal Qualification Test Activities

Traditional formal qualification test and evaluation activities include software component testing and system testing.

Software component testing is a formal black-box test conducted against the established allocated baseline. The purpose of component testing is to validate component behavior against the component's requirements.

System testing is a formal black-box test conducted against the established functional baseline. The purpose of system testing is to validate system behavior against the system's requirements.

Upon successful completion of formal qualification testing, the system's design documents and source code will

constitute the Product Baseline. The system maintainer inherits and controls the evolution of these documents during system maintenance.

B. TRADITIONAL SOFTWARE EVOLUTION

Under traditional DoD software evolution models, the maintainer applies source code development activities to support system software evolution and maintenance. The primary focus of software evolution and maintenance is to address the following:

- Software Correction. Modify system source code to correct software errors.
- Software Enhancements. Modify system source code to add, remove, or improve system capabilities or features.
- Software Adaptation. Modify system source code to adapt the product to new environments.

IV. INTEGRATED COTS COMPONENT SOLUTION EVOLUTION

A. PRE-EVOLUTION CONSIDERATIONS

> According to the old process, system requirements drove capabilities. In the new process, capabilities will drive system requirements. [Ref. 17]

This section looks at a few fundamental differences between a traditional software development process (to produce source code) and a COTS software development process (to produce an integrated COTS component solution).

1. COTS Requirements Definition

> The traditional approach is to have the requirements fixed before building the system. The best COTS-based approach is to look at the available technology and tailor requirements based on what's available. [Ref. 17]

> COTS works best in an environment of flexible requirements management. If the system is over-specified, it will be hard to find a COTS fit. [Ref. 17]

Under the traditional software development process, the Government establishes and tightly controls detailed system requirements and component sub-requirements. Under the COTS software development process, the developer must forego detailed system requirements in order to take maximum effective advantage of available market technologies and products.

To facilitate COTS component integration into military system architectures, the developer must re-think the way it

specifies requirements. DoD Regulation 5000.2-R requires the system acquisition agent to:

- Avoid Government unique requirements.
- Avoid restrictive statements of need.
- Avoid detailed specifications.

High-level, abstract system requirements specification for non-critical system behaviors allows the Government to adapt system requirements to available market technologies and products. Detailed requirements place undue constraints on the market: it is difficult to find a COTS software component that completely satisfies a set of detailed requirements [Ref. 18].

The developer must continue to specify well-defined, detailed requirements for critical system behaviors that cannot be modified to support available market technologies or products. A critical behavior is any essential capability or interface that must exist in the system to satisfy a mission need. Since detailed requirements constrain the market, critical requirements will provide the basis for all COTS component selections [Ref. 19]. As the number of detailed system requirements increase, the number of acceptable (and available) COTS components will decrease.

For both critical and non-critical system behaviors, the developer must extend system requirements to address

technology and vendor concerns. A product's underlying technology and source of supply will have a significant impact on the system's life cycle. The developer must carefully select technology and vendor requirements that satisfy long-term life cycle support goals.

2. COTS Requirements Infrastructure Support

> Significant up-front effort is required for COTS component selection and evaluation. [Ref. 19]

Under the traditional software development process, requirements specification and qualification testing are mutually exclusive activities. The Government establishes functional and allocated baselines that document system and component requirements, respectively. These baselines form the basis for all subsequent requirements qualification testing. Under the COTS software development process, requirements specification is dependent on COTS component selection and qualification.

DoD Regulation 5000.2-R identifies market research as an essential element in defining system requirements. System requirements can only be defined in conjunction with COTS component selection and evaluation [Ref. 19]. The developer must therefore establish front-end processes to support concurrent requirements definition and COTS component evaluation [Ref. 3]. This activity requires additional

infrastructure support earlier in the development process [Ref. 4].

3. COTS Architecture Considerations

> Software architecture must be suitable for component wrapping and gluing. [Ref. 19]

Under the traditional software development process, software engineers develop architecture and detailed component designs to satisfy well-defined, detailed component requirements. Architecture and detailed designs establish the basis for source code development and testing. Under the COTS software development process, architecture design is dependent on COTS component selection and qualification. COTS component architecture considerations include the following:

- Adding communicating channels between mutually exclusive COTS components that need to pass information.
- Adding desired functionality to an individual COTS component.
- Removing undesirable functionality from an individual COTS component.
- Modifying the behavior of an individual COTS component.

Requesting the vendor to modify component source code is one way the maintainer can address architecture concerns: there is a strong temptation to customize a COTS software

component by contracting with the developer to modify the source code [Ref. 4]. COTS source code modification by a vendor results in a modified off the shelf (MOTS) product. A custom developed MOTS component is typically not made available to the commercial market. The result: the MOTS component no longer tracks with the base COTS component resulting in high life-cycle evolution and support costs. A key element to successful use of COTS is to minimize the risk by accepting the COTS package as-is with minimal changes [Ref. 4].

One way to avoid MOTS is to limit COTS component modifications to configuration shells, scripts, and wrappers. Figure 2 illustrates how wrappers and glue code interact with COTS components. Wrappers and glue code provide the following benefits:

- Wrappers allow the maintainer to modify component behavior without modifying component source code.
- Wrappers allow the maintainer to add, remove, or modify component functionality.
- Glue code provides a communication channel between mutually exclusive COTS software components that need to exchange information.
- Wrappers provide an interface between an individual COTS software component and the glue code.

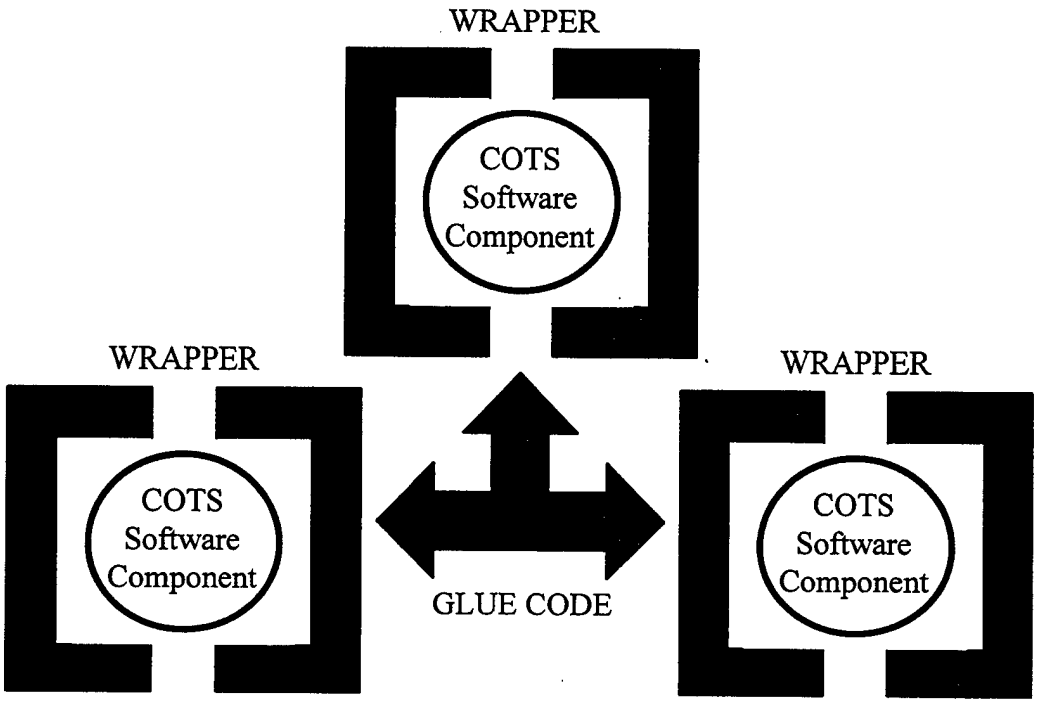

Figure 2. COTS Architecture Employing Wrappers and Glue Code.

Wrapper and glue code maintenance is achieved using traditional source code evolution activities. Acquired COTS wrappers and glue code maintenance is achieved using COTS component evolution activities. The maintainer must assess future component selections/upgrades for impact on wrapper requirements and re-engineering: should it become necessary to substitute a new or updated COTS component for an obsolete one, most of the code modifications required to support the new component will occur in the wrapper [Ref. 19].

The following Naval Postgraduate students are currently researching architecture considerations for COTS-intensive systems:

- Gee [Ref. 20] is developing an architectural framework for COTS/GOTS/legacy systems.
- Tran and Allen [Ref. 21] are addressing COTS architecture wrapper design and security implementation issues.

B. THE INTEGRATED COTS COMPONENT EVOLUTION (ICCE) MODEL

> Regardless of which lifecycle model an organization uses (waterfall, spiral, or iterative), ... the use of COTS products has a pervasive impact on all lifecycle processes. [Ref. 7]

Traditional software evolution activities focus on source code modifications to correct errors, to adapt the system to new environments, and to enhance system capabilities. For an integrated COTS component solution, the maintainer is a consumer of software instead of a source code developer. The maintainer, no longer in control of source code specification, release, and maintenance, must focus on continually adapting the system to new market technologies and products. The result: software evolution, traditionally a logical rather than a physical exercise [Ref. 22] takes on the physical characteristics of the system engineering process:

- System software is composed of a large number of parts (components).
- System software parts are developed by multiple people and contractors (vendors).
- System software is comprised of a large number of complex interfaces.
- System software cannot change easily.

System evolution, no longer able to directly affect source code modification, must now focus on the following COTS evolution activities:

- Software Addition. Add new COTS software components to the system.
- Software Removal. Remove extant COTS software components from the system.
- Software Modification. Modify extant COTS software components through component upgrades or changes in component configuration. Software modification does not include modifying a COTS component (MOTS).

Software evolution and maintenance for COTS-intensive systems require technical, organizational, and management changes. As a minimum, the maintainer must satisfy the following key elements:

- Support executable instead of source code evolution and maintenance.
- Provide proactive activities that work in a dynamic and rapidly changing market environment.
- Allow the maintainer to make quick assessments and build decisions.

- Provide formal build decision milestones.
- Support COTS component integration activities (includes wrapper and glue code development and maintenance).
- Provide strict COTS configuration management activities.

Figure 3 represents the integrated COTS component evolution (ICCE) model for COTS-based military systems. To address the key characteristics identified above, the ICCE model emphasizes the following four activities:

- Continuous Market Awareness.
- Continuous Risk Awareness.
- Continuous User Awareness.
- ICCE Test and Evaluation.

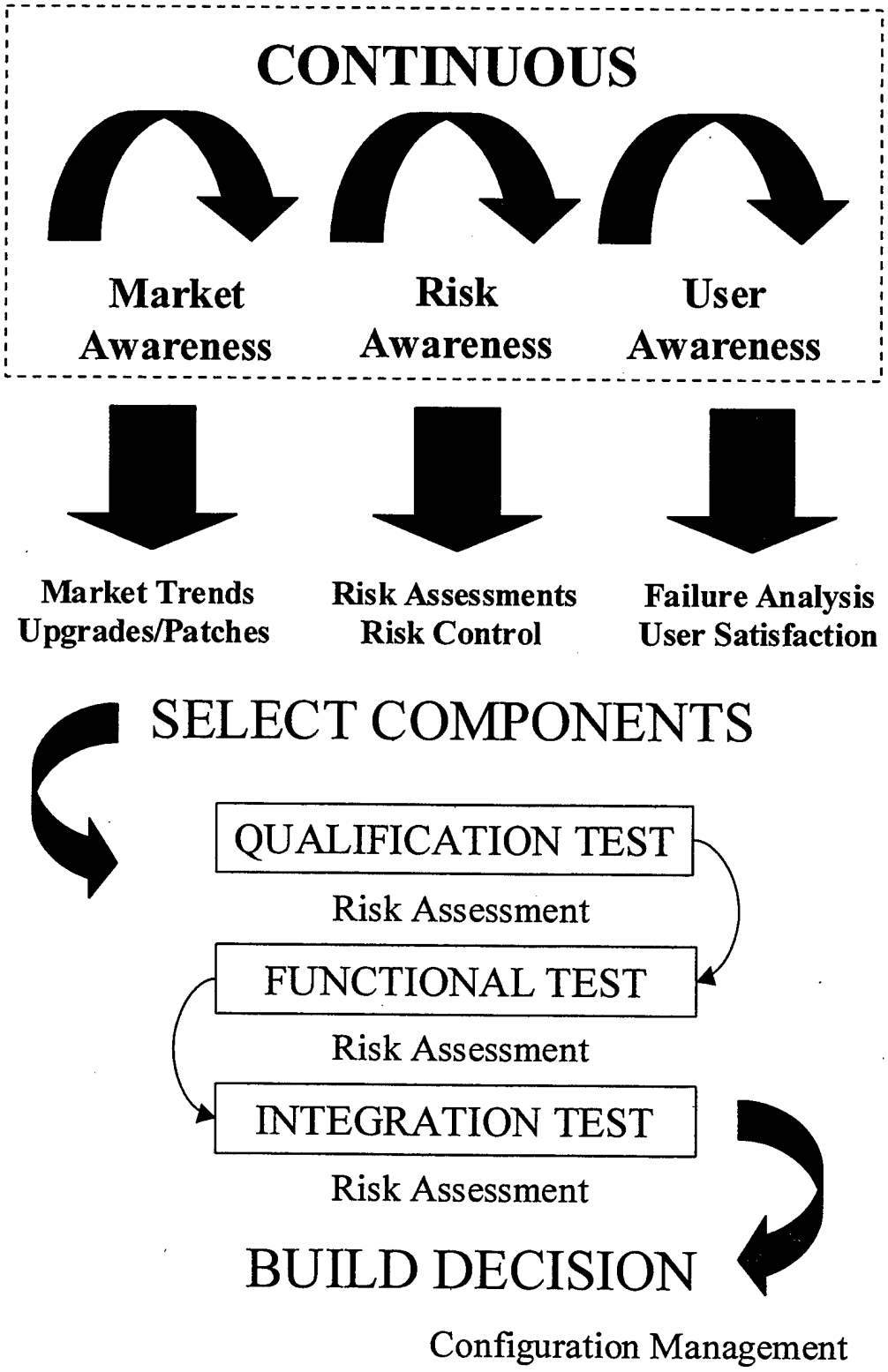

Figure 3. Integrated COTS Component Evolution (ICCE) Model.

ICCE market awareness activities monitor market trends to ensure the Government secures the optimal, cost effective component solution for its system. Continuous market awareness activities include:

- Monitor the market for emerging technologies.
- Monitor the market for new, competitive product sources (vendors).
- Monitor the market for new, emerging products.
- Monitor extant product vendors for product upgrades.
- Monitor extant technologies, vendors, products assessed as high risk.

ICCE risk awareness activities focus on extant system software components to ensure the maintainer remains informed and proactive with respect to applied problematic technologies, vendors, and products. Section IV.C.2 provides a detailed look at ICCE risk awareness activities. Continuous risk awareness activities include the following:

- Develop risk assessments for extant system software components.
- Develop risk mitigation strategies and contingency plans for high risk software components.

ICCE user awareness activities focus on user acceptance of the fielded system. As discussed in section II.C.2, an integrated component solution consists of a large number of COTS components acquired from multiple vendors. Since these

components are selected to satisfy a broad set of flexible, abstract requirements, the ultimate system success determinate will reside with the user. The maintainer must maintain awareness of user satisfaction especially with respect to system performance, robustness, capabilities, documentation, and usability. Continuous user awareness activities include the following:

- Capture software component trouble reports and perform failure analysis.
- Solicit user feedback and assess user satisfaction with the fielded system.
- Solicit user beneficial suggestions to improve system suitability and effectiveness.

ICCE test and evaluation activities validate the selected component solution against system operational requirements. Chapter VI provides a detailed look at COTS test and evaluation activities. ICCE test and evaluation activities include the following:

- Perform requirements analysis with respect to the addition, removal, and modification of system components (component qualification testing).
- Perform technology, vendor, and product risk assessments for new and modified system components (component qualification testing).
- Validate expected component behavior and capabilities for new and modified system components (component functional testing).

- Validate expected system behavior and capabilities for the proposed build (component integration and system testing).

ICCE configuration management activities focus on product baseline control (software and associated documentation), developmental data control, and market trend analysis. ICCE configuration management activities include:

- Maintain configuration control over product releases (product baseline version control).
- Maintain configuration control over risk assessment charts and risk information sheets (risk awareness product control).
- Maintain configuration control over software trouble reports and beneficial suggestions (user awareness product control).
- Maintain configuration control over software baseline change requests (test and evaluation product control).
- Establish an historical database of extant software component evolution and predict product upgrade trends.
- Maintain a library of all project development data.

C. THE ICCE PROCESS

Figure 4 provides an overview of the ICCE process. This section provides a detailed look at the following ICCE process components:

- User Awareness Process.
- Risk Awareness Process.
- Market Awareness Process.

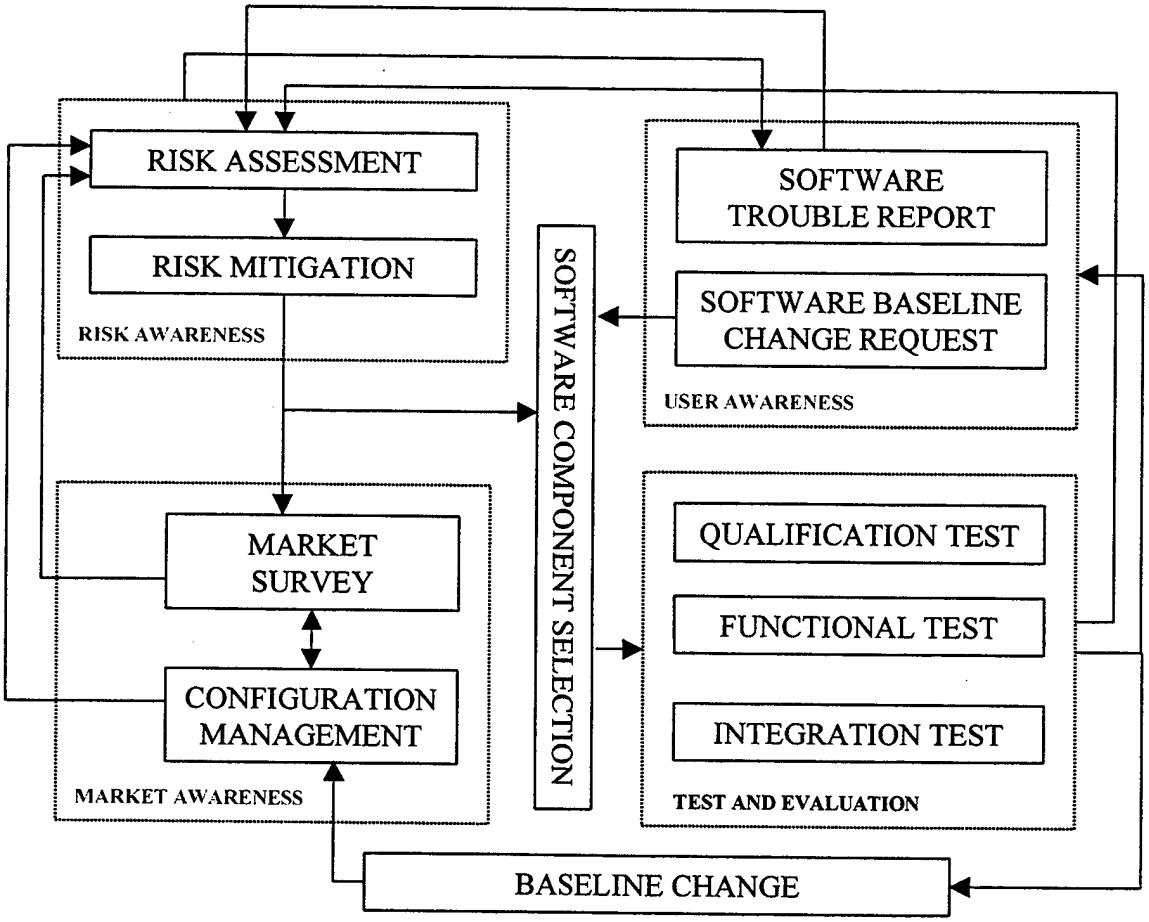

Figure 4. ICCE Process Overview.

1. ICCE User Awareness Process

Figure 5 provides a detailed view of the ICCE user awareness process. ICCE user awareness process inputs include:

- User feedback (casualty reports, trouble reports, beneficial suggestions, user satisfaction).
- Risk awareness feedback (software component risk assessments).
- COTS test and evaluation feedback (software baseline change request status).

ICCE user awareness process outputs include:

- Software component trouble reports (to risk awareness).
- Software baseline change requests (to software component selection).

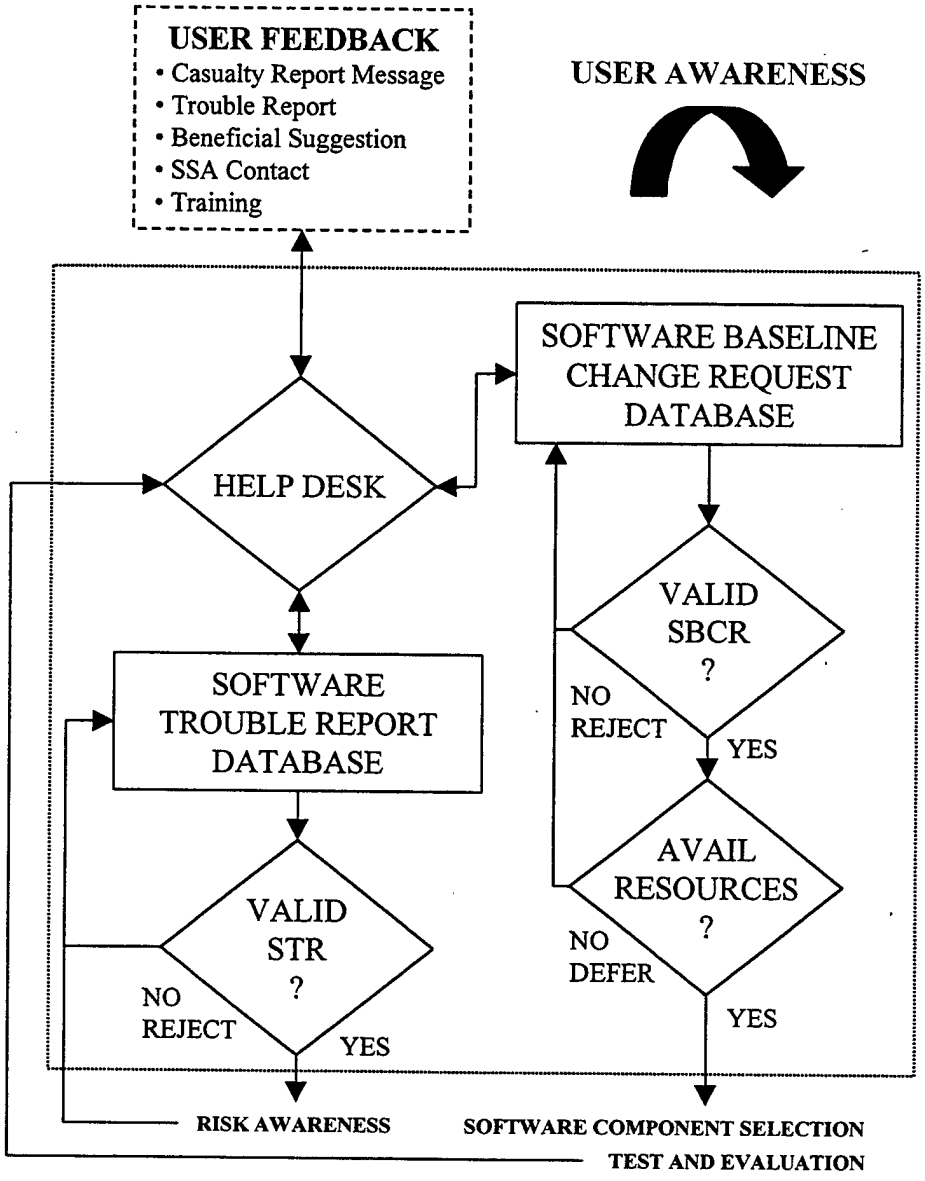

Figure 5. ICCE User Awareness Process.

Help desk. The help desk consists of system subject matter experts and provides a single point of contact to the user. The primary purpose of the help desk is to:

- Capture feedback from the user.
- Provide technical assistance to the user.
- Provide software trouble report and software baseline change request status to the user.

The help desk establishes and maintains the mechanisms to capture user feedback. Examples include the following:

- Casualty reports (official U.S. Navy message). A casualty report communicates a state of system degradation or failure that results in a reduced operational capability.
- Trouble reports (hard copy, e-mail, phone, IRC, or web-based). A trouble report typically reports a software problem that does not result in casualty report. Examples include problems with system performance, component configuration, system administration, support documentation, or system operability (ease-of-use).
- Beneficial suggestions (hard copy, e-mail, phone, IRC, or web-based). A beneficial suggestion reports a user request for new system features or capabilities.
- Indirect feedback. Indirect feedback includes informal user feedback submitted by the software maintainer or the training activity on behalf of the user.

Help Desk Technical Assistance. The maintainer provides a single point of contact to the user for fleet technical assistance (face the fleet initiative). Direct user

interaction with product vendors should be restricted. The primary reasons include:

- A COTS-intensive system consists of a large number of components supplied by a large number of vendors. The user should not have to search for the appropriate vendor help desk to resolve system problems.
- The maintainer must capture all trouble reports to perform adequate system failure analysis.
- By performing system technical assistance, the maintainer maintains a core technical capability and is able to provide better technical assistance to the user.
- The vendor may not understand the system's integrated environment.
- The vendor may alter the system's product baseline by offering new untested product software, upgrades, or patches.
- The user will not have access to all product warranty or maintenance agreement data.

The help desk creates a software trouble report (STR) entry in the STR database for each unique problem reported by the user. The help desk creates a software baseline change request (SBCR) entry in the SBCR database for each unique user request to modify the system product baseline (software, hardware, or documentation). Help desk subject matter experts routinely access the STR and SBCR databases to provide STR and SBCR disposition feedback to the user. This information can also be provided automatically through a web based interface.

Software trouble report. The software maintainer routinely accesses the STR database to assess the validity of each open STR. A valid STR is forwarded to risk awareness activities to conduct a risk assessment. An invalid STR is rejected from further consideration. The STR database is updated to reflect STR disposition and rationale.

Software baseline change request. The software maintainer routinely accesses the SBCR database to assess the validity of each open and deferred SBCR. A valid SBCR is forwarded for resource consideration. An invalid SBCR is rejected from further consideration. The SBCR database is updated to reflect SBCR disposition and rationale.

Valid SBCR resource consideration. Although an SBCR is considered valid, resources may not be available to test and evaluate the SBCR. Resource availability is dependent on the number and priority of selected components currently under evaluation for baseline change and the number of software engineers available to conduct testing. If resources are not available, the SBCR is deferred from further consideration. If resources are available, the SBCR is added to the list of software components selected for the next product baseline update. The SBCR database is updated to reflect SBCR disposition and rationale.

2. ICCE Risk Awareness Process

Figure 6 provides a detailed view of the ICCE risk awareness process. ICCE risk awareness process inputs include:

- User awareness feedback (software component trouble reports).
- Market awareness feedback (market surveys, configuration management).
- COTS test and evaluation feedback (software baseline change request status).

ICCE risk awareness process outputs include:

- Risk mitigation strategy or contingency plan (to market awareness).
- Software baseline change request (to software component selection).
- Software component risk assessments (to user awareness).

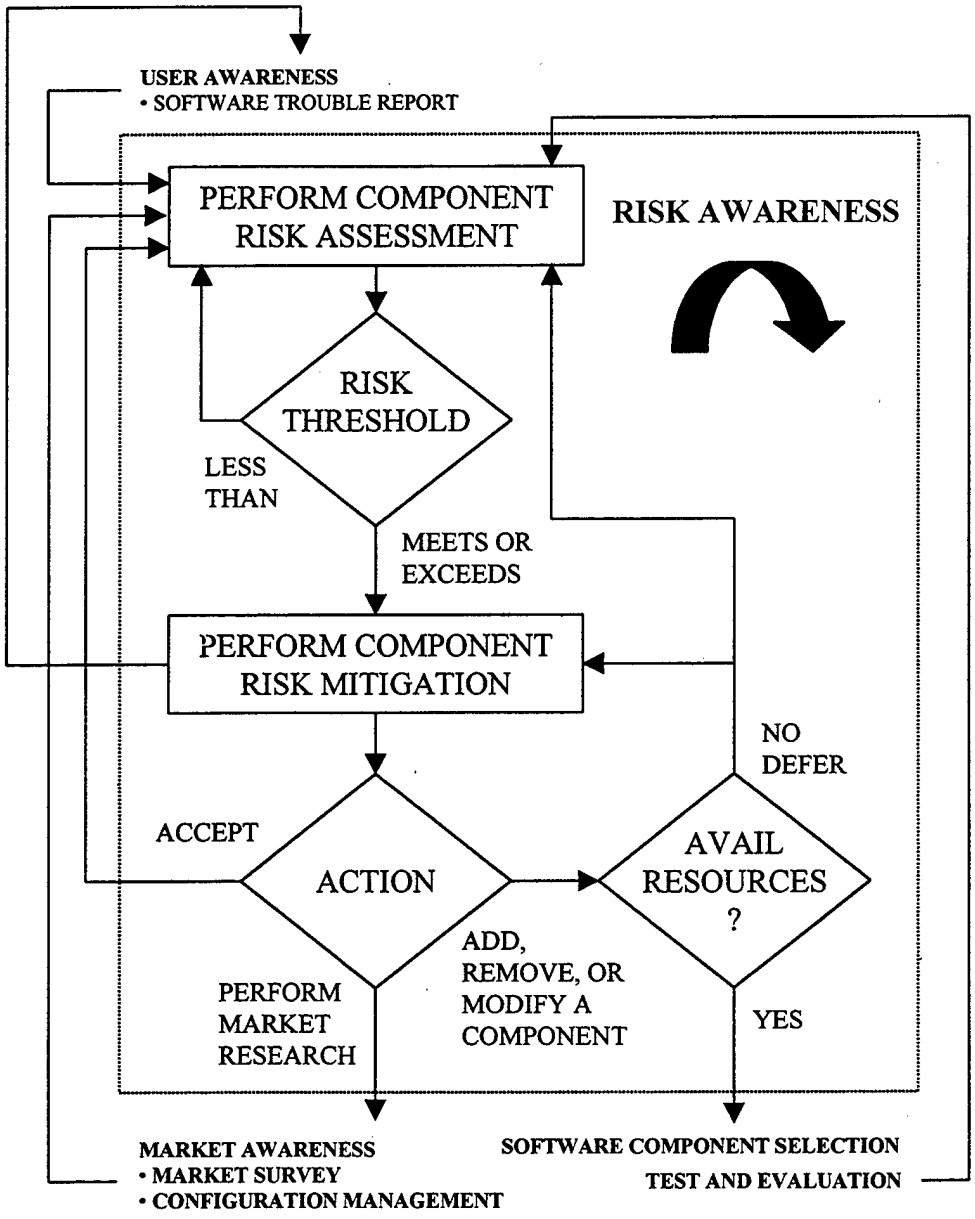

Figure 6. ICCE Risk Awareness Process.

Risk assessments. The software maintainer assesses technology, vendor, and product risks for each software component in the system. Extant component risk assessments are updated on a periodic basis to address changes in the market (market awareness feedback) and to address problems experienced in the field (user awareness feedback). The maintainer also assesses risks for software components selected for COTS test and evaluation. These include any components that impact the approved system baseline through component addition, removal, or modification.

Risk assessment threshold. Each component is evaluated against a number of risk factors. Any risk factor that meets or exceeds a predefined risk assessment rating is targeted for risk control. Risk control activities require significant resources. To avoid overwhelming these resources, the maintainer must select a risk assessment threshold that filters out low and medium risks.

Risk control. The maintainer develops a risk mitigation strategy for each component risk factor that exceeds the risk threshold. The maintainer also develops a risk contingency plan that will be triggered if the risk mitigation strategy fails to reduce the components risk.

Risk control actions. A components risk mitigation strategy or risk contingency plan may include any of the following actions:

- Market research. The maintainer forwards the risk to market awareness activities to monitor the market for additional information.
- Risk acceptance. The maintainer accepts the risk and takes no further action.
- Software baseline change request. The maintainer recommends a change to the product baseline in order to alleviate the risk. The maintainer prepares a software baseline change request. The maintainer forwards the SBCR for resource consideration.

The maintainer takes the appropriate risk action and updates risk assessment and risk control documentation to reflect the risk control disposition and rationale.

Risk control resource consideration. Although an SBCR is considered necessary to reduce component risks, resources may not be available to test and evaluate the SBCR. Resource availability is dependent on the number and priority of the selected components currently under evaluation for baseline change and the number of software engineers available to conduct testing. If resources are not available, the SBCR is deferred from further consideration. If resources are available, the SBCR is added to the list of software components selected for the next product baseline update. The maintainer updates risk assessment and risk control documentation to reflect SBCR disposition and rationale.

3. ICCE Market Awareness Process

Figure 7 provides a detailed view of the ICCE market awareness process. The ICCE market awareness process includes market survey and configuration management activities. ICCE market awareness process inputs include:

- Market feedback (e.g., solicitations, market literature, product demonstrations, past performance).
- Risk awareness feedback (risk mitigation or contingency plan).
- Product baseline change (version description document).

ICCE market awareness process outputs include:

- Market survey data (to risk awareness).
- Historical product trend data (to risk awareness).

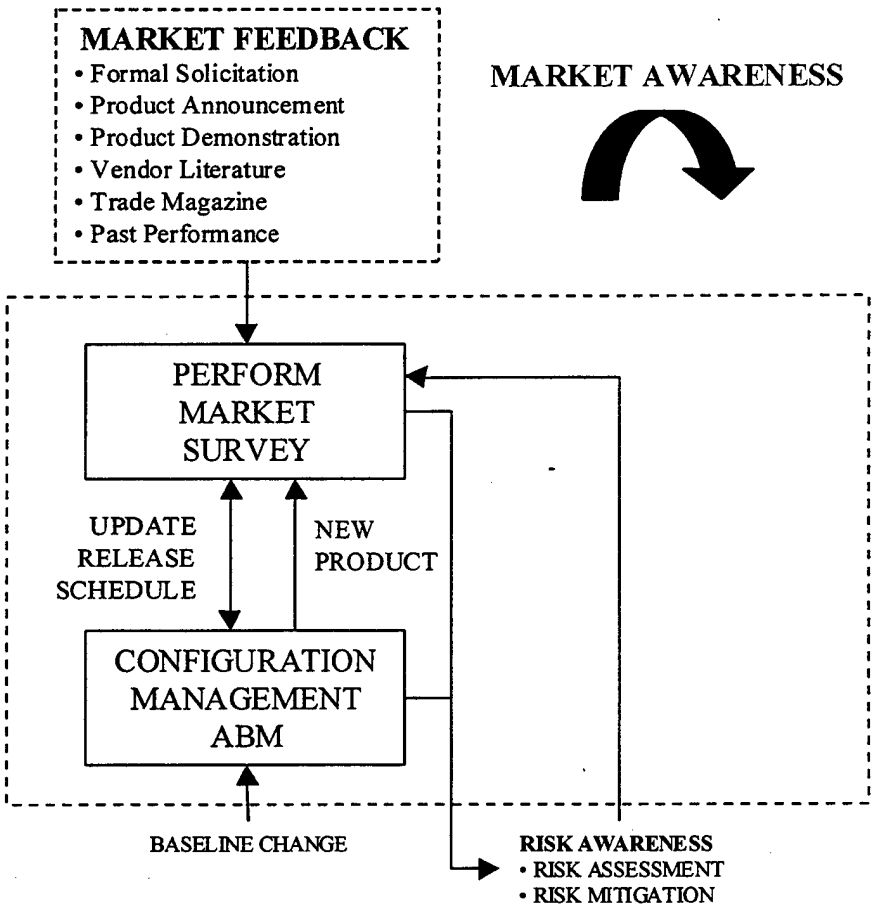

Figure 7. ICCE Market Awareness Process.

Market survey. Market survey activities include monitoring market technologies, vendors, and products to maintain a proactive awareness of market changes that may adversely impact extant system components. Market survey activities also include collecting specific information on high-risk components under risk control. High-risk market monitoring activities are conducted in accordance with the risk awareness risk mitigation strategy or contingency plan.

The market survey group establishes and maintains mechanisms to capture market feedback. Examples include the following:

- Market surveys (technology survey, product survey).
- Product announcements.
- Vendor newsletter.
- Direct vendor contact.
- Technology literature.
- Trade shows.
- Product demonstrations.
- Internet user groups.

A technology survey is a formal solicitation to collect information regarding potential market technologies available to support system requirements. A product survey is a formal solicitation to collect information on potential

market products and sources of supply available to support a particular technology.

Configuration management. Configuration management maintains formal configuration control over all software products including, but not limited to, the following:

- System product baseline (software components and associated documentation).
- User awareness documentation (software trouble reports and beneficial suggestions).
- Risk awareness documentation (risk assessment charts and risk mitigation plans).
- Test and evaluation documentation (software change request).

Configuration management establishes and maintains the ICCE library. The ICCE library contains all items under configuration control and all project-related technology, vendor, and product data.

Configuration management also establishes and maintains the ICCE activity-based model (ICCE ABM). Because the market drives the system product baseline through COTS technology and product upgrades, the maintainer must establish a proactive mechanism that captures and anticipates market changes [Ref. 28]. The ICCE ABM supports market prediction by capturing the following information for each system component:

- Component evolution (includes multiple component versions and upgrades).
- Component documentation (associated COTS documentation provided for each component evolution version/upgrade).
- Sub-component evolution (third party components).
- Component evolution availability/release dates.
- Component evolution version description document (identifies added/removed/modified capabilities-of-interest between versions/upgrades).
- Known set of incompatible COTS components [Ref. 29].

The primary goal of the ICCE ABM is to minimize the impact of market change by anticipating market trends. By anticipating market trends, the maintainer avoids getting into a reactive evolution mode. A proactive evolution mode allows the maintainer to plan for market change with consideration to alternatives. A reactive evolution mode forces product upgrades on the maintainer without consideration to alternatives. A proactive evolution mode allows the maintainer to conduct component test and evaluation in a controlled test environment. A reactive evolution mode forces component test and evaluation in the field.

V. ICCE RISK MANAGEMENT

A. CONTINUOUS RISK MANAGEMENT

> The heart of risk management is informed decision making under uncertainty. [Ref. 23]

The market is a dynamic, fluid environment subject to constant, unpredictable change. Vendor releases of COTS components arrive regularly and are difficult to re-integrate [Ref. 4]. To stay proactive in a market environment, the maintainer must establish an aggressive, systematic risk management process that continually assesses market technology, vendor, and product risks. A clear understanding of COTS component risks is essential to assess adverse market impact on system cost, schedule, and performance.

ICCE risk management applies traditional risk management activities to address the unique risks attributable to a system built around an integrated COTS component solution. ICCE risk management activities include risk assessment and risk control. Risk assessment consists of risk identification, risk analysis, and risk prioritization. Risk control consists of risk management planning, risk resolution (mitigation strategy and contingency plan), and risk monitoring.

The maintainer applies ICCE risk management activities to all extant COTS software components that comprise the system product baseline and to new software components selected for incorporation into the baseline.

ICCE risk management activities produce the following products:

- Risk Assessment Chart (RAC). Captures the risk assessment for each software component.
- Risk Summary Sheet (RSS). Provides a summary list of all risk factors assessed a high-risk rating.
- Risk Information Sheet (RIS). Captures risk control activities and status for each risk factor assessed a high-risk rating.

B. ICCE RISK FACTORS

> The DoD must sort out where the COTS is HIGH RISK and where COTS can be safely used. [Ref. 17]

This section proposes a set of COTS-based risk categories and risk factors that will be used to assess the risks for a COTS component. Risk category and risk factor selection is based on personal experience managing COTS-intensive systems. Risks are assessed against three risk categories. Each risk category has one or more risk factors. The risk categories are:

- Technology Risks.
- Vendor Risks.
- Product Risks.

1. Technology Category: Maturity/Stability Risk Factor

DoD Regulation 5000.2-R requires the DoD acquisition community to maximize effective use of industry accepted technologies. Products based on emerging technologies or unstable competing technologies will offer a higher risk to the maintainer than products based on a widely accepted technology. The major risks associated with this risk factor include:

- Buying into a technology that will not last.
- Buying into a technology that will undergo significant change.

2. Technology Category: Competition Risk Factor

DoD Regulation 5000.2-R requires the DoD acquisition community to look for multiple suppliers. Technologies with a limited product base will offer a higher risk to the maintainer than technologies with a large product base. The major risks associated with this risk factor include:

- Buying into a technology that has poor product competition.

3. Vendor Category: Maturity/Stability Risk Factor

DoD Regulation 5000.2-R requires the DoD acquisition community to address long-term product availability and supportability issues. Vendor past performance is a key

determinate for this risk factor. A vendor with a limited product line is more likely to sacrifice a product to compensate for adverse market financial flux. A vendor that employs ad-hoc development practices may not be able to sustain long-term product evolution. The major risks associated with this risk factor include:

- Buying into a vendor that will not last.
- Buying into a vendor that has a limited product line.
- Buying into a vendor that employs poor product development/maintenance practices.

4. Vendor Category: Technology Expertise Risk Factor

DoD Directive 5000.1 identifies vendor experience in the software domain or product line as a critical element for software intensive systems. The major risk associated with this risk factor includes:

- Buying into a vendor unable to adapt a product to a new environment/technology.

5. Vendor Category: Responsiveness Risk Factor

Large vendors tend to respond to market feedback while small vendors are more likely to respond directly to the individual customer (maintainer). Vendors that do not respond to any feedback offer the highest risk. Maintenance turn-around time by a vendor can also be a significant problem [Ref. 3]. Vendors that offer little or no warning

for product releases/upgrades force the maintainer into a reactive evolution mode to deal with obsolescence issues. The major risks associated with this risk factor include:

- Buying into a vendor unresponsive to customer feedback (component enhancement or corrective).
- Buying into a vendor too responsive to another customer's requirements.
- Buying into a vendor that does not announce product releases/upgrades.

6. Vendor Category: Technical Support Risk Factor

Even though a vendor provides technical assistance for a product line component, problem investigation and identification by the maintainer is the most costly part of maintenance [Ref. 3]. To support a COTS-intensive system deployed worldwide, the maintainer will require access to knowledgeable vendor technical staff 24 hours a day, 7 days a week. The major risks associated with this risk factor include:

- Buying into a vendor unable to provide adequate technical support.

7. Product Category: Market Acceptance Risk Factor

A widely accepted product with a large customer base tends to drive the market. A product with a small customer base tends to change with the market. The major risks associated with this risk factor include:

- Buying into a product that will not last.
- Buying into a product that will undergo a significant technology change.

8. Product Category: Robustness/Performance Risk Factor

Product past performance will be a major determinant for this risk factor. The ICCE ABM provides a historical record of product evolution. The major risks associated with this risk factor include:

- Buying into a product that will require a significant number of upgrades/patches.
- Buying into a product that will find poor User acceptance.

9. Product Category: Interface Risk Factor

DoD Regulation 5000.2-R requires the DoD acquisition community to specify open system objectives for military system developments. It may not be in the vendor's interest to achieve true plug and play capability. The vendor may not be willing to provide detailed interface design documentation to the vendor. The major risks associated with this risk factor include:

- Buying into a product that requires wrappers and glue code (interoperability).
- Buying into a product that will be difficult to troubleshoot (lack of interface documentation).

- Buying into a product that will be difficult to integrate (lack of interface documentation).

10. Product Category: Complexity/Features Risk Factor

ICCE user awareness activities will be a major determinant for this risk factor. The major risks associated with this risk factor include:

- Buying into a product that will require wrappers to mask undesirable features.
- Buying into a product that will find poor User acceptance (difficult to use, configure, and troubleshoot).
- Buying into a product that will require on-site load/configuration.
- Buying into a product that will require additional documentation.
- Buying into a product that will require additional training (operational, maintenance).

11. Product Category: Security Risk Factor

West-Brown and Hernan discuss how vendor interaction plays a key role in product security: although vendors provide products with built-in security features that address COTS component interoperability issues, these products are typically shipped with insecure defaults [Ref. 24]. In addition to a product's security features (and known security bugs), the maintainer must also assess and document product configuration requirements. The major risks associated with this risk factor include:

- Buying into a product that will compromise system security.

12. Product Category: Safety Risk Factor

The major risks associated with this risk factor include:

- Buying into a product that will compromise personnel safety.
- Buying into a product that will compromise equipment safety.

13. Product Category: Documentation Risk Factor

The major risks associated with this risk factor include:

- Buying into a product that will find poor User acceptance.
- Buying into a product that will require additional documentation.
- Buying into a product that will tax technical assistance resources.

14. Product Category: Cost Risk Factor

The major risks associated with this risk factor include:

- Buying into a product that exhibits expensive maintenance fees.

C. ICCE RISK ASSESSMENT CHART

The ICCE risk assessment chart (RAC) captures risk assessment data for a COTS software component. The maintainer places the initial chart and all subsequent charts under ICCE configuration control. Over time, the aggregate charts for a particular component will establish a historical risk profile. Figure 8 presents the ICCE RAC. The ICCE RAC format is based on Statz and O'Toole's risk factors chart for software process improvement [Ref. 30]. The ICCE RAC includes the following information:

- Product Name/Version: records the name and version number of the COTS component under assessment. Identify the primary component name and version number for third party components (e.g., Windows 95 4.10, Word 97 SR2).
- Assessment Date: records the date of the current risk assessment.
- Assessed By: records the name of the software engineer that performed the current risk assessment.
- Risk Category: reflects the three risk categories under evaluation.
- Risk Factors: reflects the fourteen risk factors to be assessed.
- Risk Cues: provides rating guidelines.
- Risk Rating: records a risk rating for each risk factor. The risk rating can be numeric (e.g., 0 to 10), adjective (e.g., low, medium, high), or visual (e.g., red, yellow, green).
- Notes: records supporting risk assessment rationale. Includes a unique identification number for each risk that the assessor wishes to place under risk control.

RISK ASSESSMENT CHART

Product Name/Version: | **Assessment Date:** | **Assessed By:** | **Rating**

Risk Category	Risk Factor	Risk Cues: Low	Medium	High
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.
	Safety	No safety issues.	N/A	Safety issue.
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.

NOTES:

Figure 8. ICCE Risk Assessment Chart. After Ref. [30].

D. ICCE RISK INFORMATION SHEET

The ICCE risk information sheet (RIS) captures risk analysis, control strategy and status. An RIS is prepared for each risk factor under risk control. The maintainer places all sheets (original and updates) under ICCE configuration control. Over time, the aggregate sheets will document the risk mitigation strategies, contingencies, and results for a software component. Post risk mitigation analysis will identify successful mitigation strategies for specific risks that may be applicable to other components experiencing the same risk. Figure 9 presents the ICCE RIS. The ICCE RIS is based on Dorofee, Walker, and Williams' RIS [Ref. 25]. The ICCE RIS includes the following information:

- ID: records a unique risk factor identification number (from the RAC).
- Identified: records the date the risk factor was first put under risk control.
- Risk Statement: records a brief risk statement for the risk factor. The risk statement is based on the {risk condition => risk consequence} format.
- RAC Rating: records the risk factor's risk rating (from the RAC).
- Probability: records the probability that the risk will occur (based on risk analysis). The probability rating can be adjective (Low, Medium, High), numeric (0-10), visual (Green, Yellow, Red), or a percentage (0%-100%).
- Impact: records the impact the risk will have on the program when it occurs (based on risk analysis). The impact rating can be adjective (Low, Medium, High),

numeric (0-10), visual (Green, Yellow, Red), or a percentage (0%-100%).

- Timeframe: records the projected timeframe the risk is expected to occur (based on risk analysis). The timeframe rating can be adjective (Immediate, Near, Far), numeric (0-10), visual (Green, Yellow, Red), or a percentage (0%-100%).

- Origin: records the originator of the risk rating (from the RAC).

- Assigned To: records the name of the software engineer assigned to conduct the risk analysis and formulate the risk control strategy.

- Update Date: records the date the RIS was last updated.

- Context: records additional information relevant to the risk.

- Mitigation Strategy: records specific steps that will be implemented to reduce the risk.

- Contingency Plan: records the action to be taken if the risk mitigation strategy does not reduce the risk.

- Trigger: records a date or event that triggers the contingency plan. The contingency plan overrides the mitigation plan.

- Status: records risk mitigation strategy or contingency plan status.

- Approval: records the name of the person that approves the risk mitigation strategy, contingency plan, and contingency plan trigger.

- Closing Date: records the date the risk is closed.

- Closing Rationale: records the reason the risk was closed.

ID:	RISK INFORMATION SHEET		Identified:
RAC Rating:	Statement:		
Probability:			
Impact:			
Timeframe:			
Context	Origin:	Assigned To:	Update Date:
Mitigation Strategy 1.			
Contingency Plan 1.			
Trigger:			
Status 1.			
Approval	Closing Date	Closing Rationale	

Figure 9. ICCE Risk Information Sheet. After Ref. [25].

E. ICCE RISK SUMMARY SHEET

The ICCE risk summary sheet (RSS) provides a snapshot of all risks under risk control. Figure 10 presents the ICCE RSS. The ICCE RSS is based on Dorofee, Walker, and Williams' risk spreadsheet [Ref. 25]. The ICCE RSS includes the following information:

- RAC ID: records a unique risk factor identification number (from the RAC).
- Risk Statement: records the risk statement for the risk factor (from the RAC).
- RAC Rating: records the risk factor's risk rating (from the RAC).
- Probability: records the probability that the risk will occur (from the RIS).
- Impact: records the impact the risk will have on the program when it occurs (from the RIS).
- Timeframe: records the projected timeframe the risk is expected to occur (from the RIS).
- Assigned To: records the name of the software engineer assigned to conduct the risk analysis and formulate the risk control strategy (from the RIS).
- Status: records the risk status (Open, Mitigate, Accept, and Close).

RISK SUMMARY SHEET (RSS) EXTANT		RAC Rating	Probability	Impact	Timeframe	Update Date:	
RAC ID	Risk Statement					Assigned To:	Status

•
•
•

Figure 10. ICCE Risk Summary Sheet. After Ref. [25].

THIS PAGE INTENTIONALLY LEFT BLANK

VI. ICCE RISK MANAGEMENT CASE STUDY

A. METEOROLOGICAL AND OCEANOGRAPHIC (METOC) PROGRAM EVOLUTION

From 1991 through 1997, the Tactical Environmental Support System (TESS) was the Department of the Navy's (DoN) primary METOC system. The TESS consisted of approximately 2.5M source lines of code (SLOC) running on dedicated TAC-4 computers. In 1996, Chief of Naval Operations (CNO) (N096) issued direction to replace TESS with a COTS-based, fully functional system [Ref. 26]. The replacement system, currently in development, is known as the Naval Integrated Tactical Support Subsystem (NITES). The purpose of NITES is to move DoN METOC systems towards an open architecture and to improve C4I connectivity through maximum use of off the shelf technology. The progression from TESS to NITES included fielding an interim COTS-intensive transition system called TESS Next Century Transition (TESS NC T). The TESS NC T system is currently installed on major combatant ships fleet-wide.

B. METEOROLOGICAL MOBILE FACILITY REPLACEMENT (METMF(R)) PROGRAM

The METMF(R), a meteorological system for the U.S. Marine Corps, represents a classic example of a military system acquisition based on an integrated COTS component

solution: the system is highly populated with both hardware and software COTS/GOTS components. The METMF(R) software baseline includes TESS NC T software as a GOTS component. The TESS NC T GOTS component will eventually be replaced by a NITES GOTS component.

1. METMF(R) System Description

The METMF(R) is a fully integrated system capable of automatic data acquisition from communications channels that include meteorological satellite down links, weather radar, local meteorological sensors, and remote meteorological sensors. The METMF(R) is capable of disseminating meteorological data and meteorological products via communications links and an indigenous video briefing system. The METMF(R) consists of following ten subsystems:

- Processing Subsystem (PCS).
- Communications Subsystem (CMS).
- Meteorological Satellite Subsystem (MSS).
- Rawinsonde Subsystem (RWS).
- Local Sensor Subsystem (LSS).
- Remote Sensor Subsystem (RSS).
- Video Subsystem (VDS).
- Meteorological Radar Subsystem (MRS).
- Portable Meteorological Subsystem (PMS).
- Shelter Subsystem (SSS).

2. METMF(R) System Objectives

The METMF(R) is a transportable system that provides tactical meteorological support to the Marine Air-Ground Task Force (MAGTF) in garrison and while engaged in Operations From The Sea (OFTS), Sustained Operations Ashore (SOA), and Operations Other Than War (OOTW). The METMF(R) provides the Marine Air Ground Task Force (MAGTF) with continuous meteorological observations, satellite imagery, forecasts, and other tactical decision aids and products for 30 days without re-supply. Additionally, the METMF(R) is interoperable with the Marine Corps Command and Control, Communications and Computers, and Intelligence (C^4I) systems and the Meteorological and Oceanographic (METOC) systems of the other Services and government agencies.

3. METMF(R) Hardware Overview

The METMF(R) is housed in a single International Organization for Standards (ISO) shelter that contains ten computers:

- (4) Pentium PCs running Windows NT.
- (1) Pentium PC running MS-DOS.
- (2) TAC-4 J210s running HP UNIX.
- (1) DEC Workstation running DEC UNIX.
- (1) Laptop (rugged) running Windows 95.
- (1) Laptop (rugged) running Windows NT.

4. METMF(R) Software Overview

Table 1 reflects the METMF(R) software product baseline [Ref. 27].

Type		Software	Version
COTS	Application	Internet Explorer	4.0.1 SP2
COTS	Application	Adobe Acrobat	4.0
GOTS	Application	AREPS	1.1 SR1
GOTS	Application	COMMSERVE-M	3.0
COTS	Application	Exceed	6.1
GOTS	Text File	Goodies	1.3
GOTS	Application	JMV	3.1.0.3
GOTS	Application	METCAST Client	1.1.0.3
COTS	Application	Marta	2.1.0.3c
COTS	Application	MS Office Professional 97	8.0 SR2
COTS	Application	Netscape Communicator	4.6.1
COTS	Application	Norton Antivirus	5.0
COTS	Application	PC Anywhere	8.0
GOTS	Application	SMOOS Remote and Server	3.0
GOTS	Application	WinEOTDA	1.3.3
COTS	Application	WinZip 32	7.0SR1
COTS	Application	WsFTP 32	6.0
COTS	Application	Tools-Zip NE5303	5.4
COTS	Application	CheckUPS II	3.2
COTS	Application	MB Intercept	2.7
COTS	Application	MeteorBurst	7.51
COTS	Application	Internet Information Server	2.0
COTS	Application	ARC Press	2.0
COTS	Application	ARC View	3.0B
COTS	Application	Edge	4.2
GOTS	Application	NITES II	0.5
COTS	Application	MB Data Stream Translator	2.0.3
COTS	Application	Central Data	R10.011
COTS	Application	TeraScan	3.0
COTS	Application	Panasonic First Aid Series 27	
COTS	Application	Vector Map Level 0 - SOAMAFR	3.0
COTS	Application	Vector Map Level 0 - SASAUS	3.0
COTS	Application	Vector Map Level 0 - NOAMER	4.0
COTS	Application	Vector Map Level 0 - EURNASIA	3.0
COTS	OS	DEC UNIX	4.0D
COTS	OS	HP-UX	10.20
COTS	OS	MS-DOS	6.22
COTS	OS	Windows 95	
COTS	OS	Windows NT Workstation/Server	4.0

Table 1. METMF(R) Software Product Baseline Version 1.3.

C. METMF(R) ICCE RISK ASSESSMENT

The acquisition cost for a single METMF(R) system exceeds $1M (COTS/GOTS hardware and software procurement cost only). To satisfy fiscal budget constraints, only two METMF(R) systems are acquired, integrated, and installed each year. The problem: over a one-year acquisition cycle, a significant number of METMF(R) COTS/GOTS components become obsolete. The maintainer must acquire, qualify, and integrate a significant number of new or upgraded hardware and software components for each new METMF(R) system. This pushes the maintainer into a cyclic reactive mode to constantly address integration issues, technical problems, user satisfaction concerns, and configuration management requirements. The maintainer's workload quickly outpaces available resources.

On 28 September 1999, a software risk assessment was initiated on the METMF(R) software product baseline (version 1.3). This was an initial assessment that encompassed thirty-nine COTS/GOTS components (component patches were not included in the assessment). Three METMF(R) software engineers spent a total of 80 person-hours to conduct the risk assessment. The risk assessment resulted in thirty-nine risk assessment charts (one chart for each COTS/GOTS component) and 546 risk factor ratings (39 charts, 14 risk

factors for each chart). Appendix A contains the completed risk assessment charts.

Table 2 presents the METMF(R) risk assessment results by risk factor rating.

		Risk Factor Ratings		
	TOTAL	**LOW**	**MEDIUM**	**HIGH**
Risk Factors	546	390	133	23

Table 2 METMF(R) Risk Assessment Results (by risk factor rating).

Of the 546 risk factors evaluated (by risk rating):

- 4.2% were assessed as high risk.
- 24.4% were assessed as medium risk.
- 71.4% were assessed as low risk.

Table 3 presents the METMF(R) risk assessment results by risk factor/risk category.

		Tech		Vendor				Product							
		Maturity/Stability	Competition	Maturity/Stability	Technology Expertise	Responsiveness	Technical Support	Market Acceptance	Stability/Robustness	Interfaces	Complexity/Features	Security	Safety	Documentation	Cost
Rating	LOW	28	7	27	36	19	33	29	7	32	31	30	39	33	39
	MEDIUM	11	31	12	3	18	5	10	22	7	4	4	0	6	0
	HIGH	0	1	0	0	2	1	0	10	0	4	5	0	0	0

Table 3. METMTF(R) Risk Assessment Results (by risk factor and risk category).

Of the 23 risk factors assessed as high risk (by risk category):

- 82.6% were related to product issues.
- 13.05% were related to vendor issues.
- 4.35% were related to technology issues.

Of the 23 risk factors assessed as high risk (by risk factor):

- 43.5% were related to stability/robustness issues.
- 21.7% were related to security issues.
- 17.4% were related to complexity/features issues.
- 8.7% were related to responsiveness issues.
- 4.35% were related to competition issues.
- 4.35% were related to technical support issues.

Of the 39 COTS/GOTS components evaluated, 31 were COTS components (resulting in 434 risk factors) and 8 were GOTS components (resulting in 112 risk factors). Table 4 presents the risk ratings for COTS components. Table 5 presents the risk ratings for GOTS components.

		Risk Factor Ratings		
	TOTAL	**LOW**	**MEDIUM**	**HIGH**
COTS Risk Factors	434 (100%)	331 (76.3%)	84 (19.3%)	19 (4.4%)

Table 4. METMF(R) Risk Assessment for COTS Components (by risk factor rating).

		Risk Factor Ratings		
	TOTAL	**LOW**	**MEDIUM**	**HIGH**
GOTS Risk Factors	112 (100%)	59 (52.7%)	49 (43.7%)	4 (3.6%)

Table 5. METMF(R) Risk Assessment for GOTS Components (by risk factor rating).

Even though both COTS and GOTS components reflect a similar percentage of high risks (4.4% and 3.6%, respectively), only half (52.7%) of the total GOTS component risk factors were assessed as low risk. Nearly three quarters (76.3%) of the total COTS component risk factors were assessed as low risk. The METMF(R) GOTS components tend to be mandated components with no commercial equivalent. These components may be more likely to escalate to a high risk than a COTS component.

D. METMF(R) ICCE RISK CONTROL

The METMF(R) risk assessment results were documented in a METMF(R) risk summary sheet (RSS). Since this was the initial assessment, the status of each risk was left OPEN and the risk analysis portions of the RSS were left blank. Figure 11 presents the initial METMF(R) RSS. The RSS only lists the 23 risk factors that were assessed as high risk. To address resource constraints, risk factors assessed a medium or low risk rating were not considered.

RISK SUMMARY SHEET (RSS) EXTANT		RAC Rating	Probability	Impact	Timeframe	Update Date: 15 OCT 99	
ID	Risk Statement					Assigned To:	Status
ARCPRESS 001	Y2K. VENDOR announces the ArcPress banner option, -B{file} displays the year portion of the date incorrectly when in the year 2000 or beyond. Unless a patch is installed, the METMF(R) will not be Y2K compliant.	H					OPEN
ARCVIEW 001	Y2K. VENDOR announces the ArcView License Manager diagnostic tool, FLEXlm *s lmutil* displays the incorrect date when in the year 2000 or beyond. Unless a patch is installed, the METMF(R) will not be Y2K compliant.	H					OPEN
HPUX 001	DISA recommends that the HP-UX COE baseline be updated to HP-UX 11.xx resulting in an HP-UX 11.xx DII COE 4.2 baseline. HP will drop support for HP-UX 10.20 and will be reluctant to address customer issues (Y2K, security, error corrections, etc.). HP-UX will not run on HP 750/755 platforms. Applications will need to be re-compiled to run on the HP-UX 11.xx environment.	H					OPEN
IE 001	Internet Explorer has historically been rife with bugs. There is low confidence in product robustness (including Y2K compliance) and a requirement to react to a significant number of vendor patches.	H					OPEN
IE 002	Internet Explorer has known security vulnerabilities. May impact METMF(R) system certification and accreditation or operational security.	H					OPEN
IIS 001	Internet Information Server. MWSS 271 uses ISS in lieu of NITES II Version 0.5 APACHE. ISS has known security vulnerabilities and is not DISA certified. May impact METMF(R) system certification and accreditation or operational security.	H					OPEN
MBI 001	The VENDOR is the only source for this software component. There is no acceptable alternative source. Another Vendor is willing to modify its COTS product but this would be a METMF(R) specific modification resulting in a MOTS component.	H					OPEN
MBI 002	Y2K. VENDOR announces Meteorburst Intercept version 2.7 exhibits three minor Y2K issues that may arise after 1/1/2000. None of these issues affect system operational reliability. The vendor considers these bugs as a "minor nuisance" and states they do not plan to correct.	H					OPEN
NITESII 001	NITES II 0.5 APACHE Component. NITES II is a mandated GOTS component. User feedback indicates APACHE Web Server is too complicated and confusing. The product is finding "poor" User acceptance and is taxing technical support resources.	H					OPEN
OP97SR2 001	Office Professional 97 Service Release 2 has documented security vulnerabilities that may impact system certification and accreditation.	H					OPEN
TERA 001	TERASCAN has long-standing installation and functionality problems. VENDOR continues to work issues but maintainer believes the VENDOR good be more responsive.	H					OPEN
TERA 002	TERASCAN was originally designed for the Solaris O/S. METMF(R) version runs on the HP UNIX platform. The HP customizations are not solid. Occasional lockup problems.	H					OPEN
TERA 003	TERASCAN installation is complex and difficult. VENDOR documentation has errors and omissions. File and directory post installation configuration is needed.	H					OPEN
TERA 004	TERASCAN installation procedures are not secure. A shared login is created. The METMF(R) customizations update the shared login only and are not easily portable to user accounts. No security patches are addressed. Many unnecessary services are running with security holes.	H					OPEN
JMV 001	NCT JMV. This is a mandated GOTS product bundled in TESS NC T (GOTS product). Third party Government VENDOR is unresponsive to NC T integrator. Third party VENDOR does not provide notice of product changes and support. This has caused significant impact on user operations.	H					OPEN
JMV 002	NCT JMV product undergoes significant changes.	H					OPEN
JMV 003	NCT JMV product is complex and is dependent on installation of specific COTS products. Must install client to get three files.	H					OPEN
NETSCAPE 001	NCT NETSCAPE Communicator. Customize product install to eliminate Real Player feature. Problems exist with this uninstall. Also other unnecessary features.	H					OPEN
WIN95 001	Win 95 is not secure. Configuration issues. May impact system certification and accreditation.	H					OPEN
WIN95 002	Win 95 is an old product. Product upgrade may have a significant impact on resident applications.	H					OPEN
WINNT 001	Y2K. Microsoft announces an Y2K issue exists w/Windows NT Server 4.0 SP5: the /TIMES function of the NET USER command line utility can be used to set the valid logon time for Windows NT user accounts. A s/w update will be made available for Win NT 4.0 SP 5 ASAP. The s/w upgrade will also be available in SP6. Without this upgrade, the system is not Y2K compliant	H					OPEN
WINNT 002	Preliminary system certification and accreditation report states the Windows NT configuration is essentially "out of the box". The security enhancements required by the Navy Windows NT Secure Installation and Configuration Guide are not being implemented. Unless corrected, the system will not be accredited.	H					OPEN
WSFTP 001	Y2K display problem. This is a minor problem with no impact to functionality.	H					OPEN

Figure 11. Initial METMF(R) ICCE Risk Summary Sheet.

The RSS presents an instantaneous view of assessed system risk. The RSS was presented to the program sponsor in order to establish risk control priorities. At the time of the review, Y2K was the number one priority in the military. It was agreed to assign resources to the COTS/GOTS components that had known Y2K bugs (as reported by the vendor). Resources were also assigned to a critical COTS component that was experiencing poor user acceptance in the field. The remaining risks were left open.

A risk information sheet (RIS) was prepared for each of the seven high risk factors selected for risk control. The maintainer assigned a resource to each risk to conduct risk analysis. Risk analysis included the following activities:

- Determine the probability that the risk would occur.
- Determine the impact the risk would have on the program if it occurred.
- Determine the timeframe the risk was projected to occur.
- Develop a risk control strategy to mitigate the risk.
- Develop a risk contingency plan (with an event or date trigger) that would be implemented if the risk mitigation strategy failed to alleviate the risk.

The RIS for each risk was presented to the sponsor to approve the risk mitigation strategy and contingency plan. Upon approval, the risk control activities were implemented

in accordance with the RIS. Each RIS was periodically updated to reflect status. Appendix B contains the completed risk information sheets and figure 12 presents the risk summary sheet (both updated to reflect status as of 17 NOV 99).

RISK SUMMARY SHEET (RSS) EXTANT		RAC Rating	Probability	Impact	Timeframe	Update Date: 17 NOV 99	
ID	Risk Statement					Assigned To:	Status
ARCPRESS 001	Y2K. VENDOR announces the ArcPress banner option, -B{file} displays the year portion of the date incorrectly when in the year 2000 or beyond. Unless a patch is installed, the METMF(R) will not be Y2K compliant.	M	H	L	I	Kyle Cunningham	Mitigate
ARCVIEW 001	Y2K. VENDOR announces the ArcView License Manager diagnostic tool, FLEXlm's *lmutil* displays the incorrect date when in the year 2000 or beyond. Unless a patch is installed, the METMF(R) will not be Y2K compliant.	M	H	L	I	Kyle Cunningham	Mitigate
HPUX 001	DISA recommends that the HP-UX COE baseline be updated to HP-UX 11.xx resulting in an HP-UX 11.xx DII COE 4.2 baseline. HP will drop support for HP-UX 10.20 and will be reluctant to address customer issues (Y2K, security, error corrections, etc.). HP-UX will not run on HP 750/755 platforms. Applications will need to be re-compiled to run on the HP-UX 11.xx environment.	H	H	H	F	Jan Strecker	Mitigate
IE 001	Internet Explorer has historically been rife with bugs. There is low confidence in product robustness (including Y2K compliance) and a requirement to react to a significant number of vendor patches.	H					Accept
IE 002	Internet Explorer has known security vulnerabilities. May impact METMF(R) system certification and accreditation or operational security.	H					OPEN
IIS 001	Internet Information Server. MWSS 271 uses ISS in lieu of NITES II Version 0.5 APACHE. ISS has known security vulnerabilities and is not DISA certified. May impact METMF(R) system certification and accreditation or operational security.	H					OPEN
MBI 001	The VENDOR is the only source for this software component. There is no acceptable alternative source. Another Vendor is willing to modify its COTS product but this would be a METMF(R) specific modification resulting in a MOTS component.	H					OPEN
MBI 002	Y2K. VENDOR announces Meteorburst Intercept version 2.7 exhibits three minor Y2K issues that may arise after 1/1/2000. None of these issues affect system operational reliability. The vendor considers these bugs as a "minor nuisance" and states they do not plan to correct.	H					Accept
NITESII 001	NITES II 0.5 APACHE Component. NITES II is a mandated GOTS component. User feedback indicates APACHE Web Server is too complicated and confusing. The product is finding "poor" User acceptance and is taxing technical support resources.	H					OPEN
OP97SR2 001	Office Professional 97 Service Release 2 has documented security vulnerabilities that may impact system certification and accreditation.	H					OPEN
TERA 001	TERASCAN has long-standing installation and functionality problems. VENDOR continues to work issues but maintainer believes the VENDOR good be more responsive.	H	H	H	I	Kyle Cunningham	Mitigate
TERA 002	TERASCAN was originally designed for the Solaris O/S. METMF(R) version runs on the HP UNIX platform. The HP customizations are not solid. Occasional lockup problems.	H					OPEN
TERA 003	TERASCAN installation is complex and difficult. VENDOR documentation has errors and omissions. File and directory post installation configuration is needed.	H					OPEN
TERA 004	TERASCAN installation procedures are not secure. A shared login is created. The METMF(R) customizations update the shared login only and are not easily portable to user accounts. No security patches are addressed. Many unnecessary services are running with security holes.	H					OPEN
JMV 001	NCT JMV. This is a mandated GOTS product bundled in TESS NC T (GOTS product). Third party Government VENDOR is unresponsive to NC T integrator. Third party VENDOR does not provide notice of product changes and support. This has caused significant impact on user operations.	H	H	H	N	Kyle Cunningham	Mitigate
JMV 002	NCT JMV product undergoes significant changes.	H					OPEN
JMV 003	NCT JMV product is complex and is dependent on installation of specific COTS products. Must install client to get three files.	H					OPEN
NETSCAPE 001	NCT NETSCAPE Communicator. Customize product install to eliminate Real Player feature. Problems exist with this uninstall. Also other unnecessary features.	H					OPEN
WIN95 001	Win 95 is not secure. Configuration issues. May impact system certification and accreditation.	H					OPEN
WIN95 002	Win 95 is an old product. Product upgrade may have a significant impact on resident applications.	H					OPEN
WINNT 001	Y2K. Microsoft announces an Y2K issue exists w/Windows NT Server 4.0 SP5: the TIMES function of the NET USER command line utility can be used to set the valid logon time for Windows NT user accounts. A s/w update will be made available for Win NT 4.0 SP 5 ASAP. The s/w upgrade will also be available in SP6. Without this upgrade, the system is not Y2K compliant	H	H	M	I	Kyle Cunningham	Mitigate
WINNT 002	Preliminary system certification and accreditation report states the Windows NT configuration is essentially "out of the box". The security enhancements required by the Navy Windows NT Secure Installation and Configuration Guide are not being implemented. Unless corrected, the system will not be accredited.	H					OPEN
WSFTP 001	Y2K display problem. This is a minor problem with no impact to functionality.	M	H	M	I	Kyle Cunningham	Mitigate

Figure 12. METMF(R) ICCE Risk Summary Sheet.

E. METMF(R) RISK MANAGEMENT CASE STUDY CONCLUSIONS

The ICCE risk management process is an effective way to identify, prioritize, and control METMF(R) system risks. Prior to the ICCE risk assessment, the maintainer, operating in a reactive mode, was unable to effectively address the growing number of COTS product, vendor, and technology issues:

- COTS software issues were addressed in an ad-hoc manner and a number of significant issues were not mitigated.
- The maintainer was installing product upgrades and patches in the field without test and evaluation.
- The user was installing unauthorized software (product upgrades, patches and other software) to address unresolved software issues.
- User satisfaction was deteriorating due to poor system performance and inadequate support documentation (load procedures, operator's manuals).
- Software configuration control was not able to keep up with all the software baseline changes.
- All the above resulted in an increase number of technical assistance requests.
- Software resources were stretched thin and personnel moral was low.

After ICCE risk assessment, the maintainer was able to accomplish the following:

- Quantify COTS product, vendor, and technology risks.
- Effectively allocate resources to address high priority risks.

- Add, remove, and modify software baseline components in a structured, disciplined manner.
- Provide sponsor visibility into the risks under risk control.
- Provide sponsor visibility into the risks NOT under risk control.
- Obtain sponsor *buy-in* into the COTS evolution process (the sponsor assigns risk priorities and approves risk mitigation strategies and contingency plans).
- Maintain software baseline configuration control.

The ICCE risk management process provided excellent sponsor insight into the overwhelming number of significant software issues surrounding the METMF(R) program. As a result of the risk assessment, an additional software engineer was added to support risk mitigation. Currently, the maintainer has mitigated the identified Y2K issues and is now addressing system security certification and accreditation issues.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. ICCE TEST AND EVALUATION

A. ICCE TEST AND EVALUATION OVERVIEW

The primary purpose of traditional qualification test and evaluation is to accomplish the following activities:

- Validate component behavior against detailed component requirements (allocated baseline).
- Validate system behavior against detailed system requirements (functional baseline).

For a system built around an integrated COTS component solution, the maintainer must expand the traditional test and evaluation role to address the following:

- The test and evaluation process must validate component/system behaviors against detailed and abstract requirements (refer to Subsection IV.A.1).
- The test and evaluation process must support concurrent component evaluation and requirements specification (refer to Subsection IV.A.2).
- The test and evaluation process must support architecture issues including script, wrapper, and glue-code development and test (refer to Subsection IV.A.3).
- In addition to product qualification, the test and evaluation process must qualify the products source-of-supply and underlying technology.

The ICCE test and evaluation process provides test and evaluation activities for COTS-intensive systems. The purpose of ICCE test and evaluation is to assess the costs

and benefits (tangible and intangible) associated with a software baseline change. The ICCE test and evaluation process includes the following three major activities:

- Qualification test and evaluation.
- Functional test and evaluation.
- Integration test and evaluation.

Qualification test and evaluation is a paper study to assess risk and requirements impact. The maintainer investigates the product, the products source-of-supply, and the products underlying technology. The maintainer develops functional test criteria for products that pass qualification testing.

Functional test and evaluation is a product study to assess product behavior in terms of desired and undesired functionality. The maintainer conducts product functional testing in a stand-alone, non-integrated test environment. The maintainer develops integration test criteria for products that pass functional testing.

Integration test and evaluation is a system study to assess product and system behavior in a fully integrated test environment representative of an operational system. The maintainer conducts integration testing on all products approved for integration testing. The maintainer includes user involvement to assess user satisfaction.

B. ICCE QUALIFICATION TEST AND EVALUATION

> As new versions of components are released by the software developers, and as superior components become available in the marketplace, system maintainers must evaluate the costs and benefits of integrating newer versions of the component into the system. [Ref. 19]

The primary purpose of qualification test and evaluation is to assess risk and requirements impact.

1. ICCE Qualification Test and Evaluation Inputs

ICCE qualification test and evaluation includes the following inputs:

- Software component selection list.
- System requirements matrix.
- Component risk assessment charts (for extant baseline components).

The software component selection list consists of one or more software components and a baseline change recommendation for each component. The list is populated by ICCE user and risk awareness activities: user awareness activities identify software components in response to beneficial suggestions (user feedback) and risk awareness activities identify software components in response to risk mitigation strategies/contingency plans (risk control). A baseline change recommendation includes any of the following actions:

- Software Addition. Add a new COTS software component to the system.
- Software Removal. Remove an existing COTS software component from the system.
- Software Modification. Modify an existing COTS software component through component upgrade or configuration change.

The system requirements matrix consists of the following information:

- Complete set of system detailed (critical) and abstract (non-critical) requirements.
- A mapping of system components to system requirements.

The component risk assessment chart (RAC) contains the current risk assessment for an existing baseline component. The risk awareness process provides a RAC for each component subject to baseline removal or modification.

2. ICCE Qualification Test and Evaluation Activities

ICCE qualification test and evaluation includes the following activities:

- Perform component qualification testing.
- Prepare a qualification test report.
- Develop a functional test plan.

Component qualification testing consists of the following:

- Component risk assessment.
- Requirements analysis.

The maintainer performs component risk assessments to evaluate product, vendor, and technology risks. Risk assessment results are documented in an ICCE RAC. The maintainer develops a new RAC for components selected for baseline addition. The maintainer updates existing charts for components selected for baseline removal or modification. Section V presents product, vendor, and technology risk factors. The following represents typical investigation questions:

- Is the product based on a stable technology?
- Are there a reasonable number of competing products?
- How often does the vendor release product upgrades and patches?
- Does the vendor offer advance notice for product upgrades and patches?
- Does the vendor respond to customer feedback?
- Does the vendor offer adequate product technical assistance?
- Has the vendor been in business for a long time?
- Does the product have any known bugs (e.g., security, Y2K)?

- Does the product have adequate support documentation?
- Does the product offer the desired capabilities?
- Does the product offer undesired capabilities?
- Does the product use proprietary interfaces?

The maintainer performs requirements analysis to accomplish the following:

- Assess system requirements impact.
- Determine component requirements.

The maintainer documents requirements analysis results in a component requirements profile. The component requirements profile includes the following information:

- System requirements impact (includes updated system requirements matrix).
- Component architecture requirements (includes scripts, wrappers, glue-code).
- Component configuration requirements.
- Component documentation requirements (includes new or supplemental support documentation).
- Component training requirements.

The maintainer documents qualification test results (risk assessment and requirements analysis) in a qualification test report. The qualification test report

updates the baseline change recommendation for each component under evaluation.

Based on the qualification test report, the maintainer prepares a functional test plan. The functional test plan provides the basis for functional testing and includes the following information:

- Functional test schedule.
- Functional test resources (includes personnel and equipment).
- Functional test environment (includes equipment configuration).
- Functional test cases.
- Functional test procedures.
- Expected test results.
- Acceptable test results.

3. ICCE Qualification Test and Evaluation Outputs

ICCE qualification test and evaluation includes the following outputs:

- Component risk assessment charts.
- Component requirements profile (includes an updated system requirements matrix).
- Qualification test report.
- Functional test plan.

C. ICCE FUNCTIONAL TEST AND EVALUATION

> Extensive evaluation of the COTS component will be required to ensure not only that the component has the functionality to perform the required tasks within the system, but also that the additional functionality inherent within the component does not interfere with the system. [Ref. 4]

The primary purpose of functional test and evaluation is to assess product behavior.

1. ICCE Functional Test and Evaluation Inputs

ICCE functional test and evaluation includes the following inputs:

- Component risk assessment charts.
- Component requirements profile.
- Qualification test report.
- Functional test plan.

2. ICCE Functional Test and Evaluation Activities

> Determining behaviour of COTS software components is difficult. [COTS] documentation, no matter how well done, is insufficient for understanding the detailed behaviour of components. [Ref. 4]

ICCE functional test and evaluation includes the following activities:

- Perform component functional testing.
- Develop supplemental documentation.
- Prepare a functional test report.

- Update component risk assessment charts.
- Update component risk profile.
- Develop an integration test plan.

The maintainer performs component functional testing in accordance with the functional test plan. Functional test and evaluation includes the following goals:

- Validate desirable component behavior (capabilities, robustness, performance, complexity).
- Validate component documentation.
- Validate component configuration.
- Identify undesirable component behavior.

The maintainer develops supplemental documentation to support the baseline change request. The following includes example documentation requirements:

- Preliminary component load procedures and configuration parameters for a baseline addition or modification.
- Preliminary component uninstall procedures for a baseline removal.
- Preliminary operating procedures (supplements COTS component operation in the integrated environment).
- Preliminary training material.
- Preliminary change pages to system documents affected by the baseline change request.

The maintainer documents functional test results in a functional test report. The functional test report updates the baseline change recommendation for each component under evaluation.

Based on the functional test report, the maintainer updates component risk assessment charts, updates the component requirements profile, and prepares an integration test plan. The integration test plan provides the foundation for integration testing and includes the following information:

- Integration test schedule.
- Integration test resources (includes personnel and equipment).
- Integration test environment (includes equipment configuration).
- Integration test cases.
- Integration test procedures.
- Expected test results.
- Acceptable test results.

3. ICCE Functional Test and Evaluation Output

ICCE functional test and evaluation includes the following outputs:

- Updated component risk assessment charts.
- Updated component requirements profile (includes an updated system requirements matrix).

- Supplemental documentation.
- Qualification test report.
- Functional test report.
- Integration test plan.

D. ICCE INTEGRATION TEST AND EVALUATION

> The primary task in maintenance of COTS software based systems involves solving integration problems as opposed to changing internal code of components. [Ref. 19]

The primary purpose of integration test and evaluation is to assess product and system behavior in an integrated environment.

1. ICCE Integration Test and Evaluation Inputs

ICCE integration test and evaluation includes the following inputs:

- Component risk assessment charts.
- Component requirements profile.
- Supplemental documentation.
- Qualification test report.
- Functional test report.
- Integration test plan.

2. ICCE Integration Test and Evaluation Activities

ICCE integration test and evaluation includes the following activities:

- Develop/acquire integration components (includes scripts, wrappers, glue-code)
- Perform integration testing.
- Update supplemental documentation.
- Prepare an integration test report.
- Update component risk assessment charts.
- Update component requirements profile.

The maintainer develops or acquires integration components to allow the component to operate in the system's integrated environment. The following includes example integration components:

- Wrappers to mask undesirable component functionality.
- Wrappers to add desirable component functionality.
- Wrappers and glue-code to add communication channels between mutually exclusive components.
- Scripts to automatically set component configuration parameters.

The maintainer performs integration testing in accordance with the integration test plan. To assess user satisfaction, integration test and evaluation involves user

participation and feedback. Integration test and evaluation includes the following goals:

- Validate desirable component behavior in the integrated environment (capabilities, robustness, performance, complexity, and interfaces).
- Validate integration component effectiveness.
- Validate supplemental documentation (load procedures, uninstall procedures, component and related system manuals).
- Identify undesirable component/system behaviors.
- Assess user acceptance.

The maintainer documents integration test results in an integration test report. The integration test report provides a final baseline change recommendation for each component under evaluation.

Based on the integration test report, the maintainer updates the component risk assessment charts, the component requirements profile, and the supplemental documentation.

3. ICCE Integration Test and Evaluation Outputs

ICCE integration test and evaluation includes the following outputs:

- Updated component risk assessment charts.
- Updated component requirements profile (includes an updated system requirements matrix).
- Updated supplemental documentation.
- Qualification test report.

- Functional test report.
- Integration test report (includes final baseline change recommendation with supporting rationale).

VIII. CONCLUSIONS AND RECOMMENDATION

A. CONCLUSIONS

Department of Defense (DoD) acquisition policy requires that military system acquisitions incorporate commercial-off-the-shelf (COTS) components into system architectures. Traditional DoD source-code development and evolution methodologies do not effectively support COTS-intensive systems. To fully realize the benefits of COTS products and technologies, the DoD must adopt new ways to sustain system evolution in the face of a dynamic market environment subject to constant change.

This thesis proposes a new software evolution model to effectively maintain COTS-intensive military systems. The integrated COTS component evolution (ICCE) model provides evolution processes designed to support the maintainer as a consumer of software instead of a source-code developer. The ICCE model achieves the following major goals:

- Support executable instead of source-code evolution and maintenance.
- Provide proactive activities that work in a dynamic and rapidly changing market environment.
- Allow the maintainer to make quick component assessments and build decisions.
- Provide formal evolution decision milestones.

- Provide a COTS test and evaluation process conducive to system composed of COTS components.

The ICCE model provides proactive risk awareness, market awareness, and user awareness activities along with a three-tier test and evaluation process.

1. ICCE Risk Awareness Process

To stay proactive in a constantly changing market environment, the maintainer of a COTS-intensive system must be able to recognize and control market-driven risks. The ICCE risk awareness process provides continuous risk awareness activities designed to identify, quantify, and mitigate product, vendor, and technology risks. A case study for the U.S. Navy/Marine Corps Meteorological Mobile Facility Replacement (METMF(R)) demonstrates the effectiveness of the ICCE risk awareness process.

2. ICCE Market Awareness Process

Market research is an essential element in defining system requirements [Ref. 11]. The ICCE market awareness process provides continuous market awareness activities to ensure the maintainer secures the optimal cost effective component solution. Market awareness activities look for emerging technologies, new products, and new sources-of-supply (vendors). The maintainer adapts system requirements to the market in order to take full advantage of available (and desirable) products and technologies.

The market affects system evolution through product, vendor, and technology changes. To minimize adverse market fluctuations, the ICCE market awareness process provides proactive activities to capture market change data for all extant system components. This data provides a component historical record and allows the maintainer to establish market trends and anticipate market changes.

3. ICCE User Awareness Process

The integrated COTS component solution consists of a large number of COTS products acquired from multiple vendors. System products are selected to satisfy a broad set of flexible abstract requirements. Since these products, along with their underlying technologies and sources-of-supply, reflect varying levels of quality, the ultimate system success determinant resides with the user. The ICCE user awareness process provides continuous user awareness activities to capture user feedback especially with respect to system performance, robustness, capabilities, documentation, and usability. User awareness activities capture software trouble reports, provide system technical assistance, perform component failure analysis, and capture user beneficial suggestions.

4. ICCE Test and Evaluation Process

A test and evaluation process for a COTS-intensive system must support the following COTS evolution activities:

- add new software components to the system baseline
- remove extant software components from the system baseline
- modify the system baseline through component upgrades or changes to component configurations

The ICCE model provides a three-tier ICCE test and evaluation process designed to eliminate inadequate baseline change proposals prior to expensive integration testing.

The ICCE qualification test and evaluation process provides activities to assess product, vendor, and technology risks. Since system requirements can only be defined in conjunction with component selection [Ref. 19], the ICCE qualification test and evaluation process also includes concurrent component selection and requirements specification activities.

The ICCE functional test and evaluation process provides activities to assess product behavior in terms of desired and undesired functionality. Each product is evaluated in a stand-alone, non-integrated environment.

The ICCE integration test and evaluation process provides activities to assess product and system behavior in a fully integrated environment representative of an operational system. The maintainer includes user involvement to assess user satisfaction.

B. RECOMMENDATIONS

> Currently there is little data on the cost, schedule, or quality benefits of COTS based systems. [Ref. 7]

To be successful, the integrated COTS component evolution (ICCE) model must provide cost effective software evolution processes and activities for a wide variety of military systems. As the number of COTS-intensive military systems increase, new software evolution strategies will surface. Incorporating lessons-learned by other Department of Defense (DoD) organizations can further optimize the ICCE model:

- Identify emerging DoD software evolution processes and activities for COTS-intensive military systems.
- Quantify software evolution performance (i.e., rate the degree of success for each evolution strategy).
- Capture associated cost and schedule data.
- Correlate successful software evolution performance to COTS component architecture.
- Establish an evolution process repository to promote successful process reuse for other organizations.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A
METMF(R) RISK ASSESSMENT CHARTS

RISK ASSESSMENT CHART

Product Name/Version:

Acrobat Reader 4.0

Assessment Date: October 1, 1999

Assessed By: Kyle Cunningham

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	L
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	M
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	M
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

RISK ASSESSMENT CHART

Product Name/Version:	Assessment Date:	Rating
ArcPress 2.0	October 1, 1999	
	Assessed By: Kyle Cunningham	

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	L
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	M
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	H
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:
ARCPRESS001. Stability/Robustness. Display bug (Y2K) requires ArcPress 2.0 patch.

RISK ASSESSMENT CHART

Product Name/Version:

ArcView 3.0b

Assessment Date: October 1, 1999

Assessed By: Kyle Cunningham

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	L
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	M
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	H
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

ARCVIEW001. Stability/Robustness. Display bug (Y2K) with license. Requires lmutil 6.0i or greater.

RISK ASSESSMENT CHART

Product Name/Version:

AREPS 1.1 SR1

Assessment Date: October 4, 1999

Assessed By: Donald T. Gates

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	M
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	M
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	L
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	M
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	M
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	M
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	M
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

RISK ASSESSMENT CHART

Product Name/Version:

CheckUPS II 3.2

Assessment Date: October 4, 1999

Assessed By: Donald T. Gates

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	L
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	L
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	M
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	M
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

RISK ASSESSMENT CHART

Product Name/Version:

DEC Unix 4.0D

Assessment Date: October 5, 1999

Assessed By: Kyle Cunningham

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	L
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	M
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	M
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	M
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

RISK ASSESSMENT CHART

Product Name/Version:

Edge 4.2

Assessment Date: October 4, 1999

Assessed By: Kyle Cunningham

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	L
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	M
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	M
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	M
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

RISK ASSESSMENT CHART

Product Name/Version:	Assessment Date:	Rating
Exceed 6.1	October 5, 1999	
	Assessed By: Donald T. Gates	

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	L
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	L
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	L
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

RISK ASSESSMENT CHART

Product Name/Version:

HPUX 10.20

Assessment Date: October 5, 1999

Assessed By: Kyle Cunningham

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	L
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	M
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	H
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	M
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	M
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	M
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

HPUX001. Tech Support for HPUX 10.20 is being phased out.

RISK ASSESSMENT CHART

Product Name/Version:

Internet Explorer 4.0.1 SP2

Assessment Date: October 5, 1999

Assessed By: Donald T. Gates

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	L
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	L
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	H
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	H
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

IE001. Stability/Robustness. This product has historically been rife with bugs.

IE002. Security. Known security holes that may impact system certification and accreditation.

NOTE: This version of IE was required to make Win 95 Y2K compliant and was provided along with the Y2K update to the OS.

RISK ASSESSMENT CHART

Product Name/Version:

Internet Information Server 2.0

Assessment Date: October 5, 1999

Assessed By: Donald T. Gates

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	M
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	L
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	L
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	M
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	H
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

ISS001. Stability/Robustness. This S/W pkg has had (and continues to have) many bugs.

NOTE: Users are using this product instead of the mandated NITES II Apache product. Apache is complex and difficult to use.

RISK ASSESSMENT CHART

Product Name/Version:

MeteorBurst Data Stream Translator 2.0.3

Assessment Date: October 5, 1999

Assessed By: Donald T. Gates

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	M
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	M
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	L
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	M
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	M
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

RISK ASSESSMENT CHART

Product Name/Version:

MeteorBurst Intercept 2.7

Assessment Date: October 5, 1999

Assessed By: Donald T. Gates

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	M
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	H
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	M
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	M
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	M
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	H
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

MBI001. Competition. Meteor Communications Corp is the only source for this product.

MBI002. Stability/Robustness. Intercept has known bugs (leap year) that are considered no impact to ops. MCC does not plan to correct.

RISK ASSESSMENT CHART

Product Name/Version:

MeteorBurst 7.51

Assessment Date: October 5, 1999

Assessed By: Donald T. Gates

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	M
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	M
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	L
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	M
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	M
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

RISK ASSESSMENT CHART

Product Name/Version:

MARTA 2.1.0.3c

Assessment Date: October 5, 1999

Assessed By: Donald T. Gates

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	M
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	L
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	M
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

RISK ASSESSMENT CHART

Product Name/Version:

MS-DOS 6.22

Assessment Date: October 5, 1999

Assessed By: Donald T. Gates

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	L
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	M
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	L
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

RISK ASSESSMENT CHART

Product Name/Version:

NITES II 0.5

Assessment Date: October 4, 1999

Assessed By: Kyle Cunningham

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	M
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	L
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	M
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	M
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	H
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	M
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

NITESII001. Complexity/Features. Mandated GOTS product. Web Server (APACHE) is difficult to use and configure.

RISK ASSESSMENT CHART

Product Name/Version:

Norton Antivirus 5.0

Assessment Date: October 4, 1999

Assessed By: Kyle Cunningham

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	L
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	L
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	M
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	M
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

RISK ASSESSMENT CHART

Product Name/Version:

MS Office Professional 8.0 SR2

Assessment Date: October 5, 1999

Assessed By: Donald T. Gates

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	L
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	L
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	L
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	M
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	H
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

OP9SR2001. Security. Microsoft products have been historically vulnerable to security attacks and have been used as a tool for delivering viruses. May impact system certification and accreditation.

RISK ASSESSMENT CHART

Product Name/Version:

Panasonic First Aid Series 27

Assessment Date: October 5, 1999

Assessed By: Donald T. Gates

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	L
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	L
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	L
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	L
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

RISK ASSESSMENT CHART

Product Name/Version:

PC Anywhere 8.0

Assessment Date: October 5, 1999

Assessed By: Donald T. Gates

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	L
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	L
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	L
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	L
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

RISK ASSESSMENT CHART

Product Name/Version:

Central Data R10.011

Assessment Date: October 4, 1999

Assessed By: Donald T. Gates

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	M
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	L
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	L
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	M
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	L
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

RISK ASSESSMENT CHART

Product Name/Version:

TeraScan 3.0

Assessment Date: September 28, 1999

Assessed By: Lorraine Smith

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	M
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	M
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	M
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	H
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	M
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	M
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	H
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	M
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	H
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	H
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	M
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

TERA001. Responsiveness. Long standing installation problems and degraded critical functionality.

TERA002. Stability/Robustness. S/W is designed for the SOLARIS O/S. The HPUX customizations are not solid and cannot be reloaded. Occasional lockup problems.

TERA003. Complexity/Features. The installation of HPUX and TeraScan is complex. The documentation has errors and omissions. Post installation configuration by setting up files and directories is need and should be included in the installation.

TERA004. Security. The installation procedures are not secure. A shared login is created. The METMF(R) customizations update only the shared login and are not easily portable to user accounts. No security patches are addressed and many services are running that are unnecessary and have security holes.

RISK ASSESSMENT CHART

Product Name/Version:

Transition 1.3 (Commserve-M 3.0)

Assessment Date: September 28, 1999

Assessed By: Lorraine Smith

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	M
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	M
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	L
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	M
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	M
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	M
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	M
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	M
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	M
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

RISK ASSESSMENT CHART

Product Name/Version:

Transition 1.3 (Goodies 1.3)

Assessment Date: September 28, 1999

Assessed By: Lorraine Smith

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	L
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	M
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	L
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	M
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	M
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

RISK ASSESSMENT CHART

Product Name/Version:

Transition 1.3 (JMV 3.1.0.3)

Assessment Date: September 28, 1999

Assessed By: Lorraine Smith

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	M
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	M
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	H
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	H
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	M
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	H
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	M
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

JMV001. Responsiveness. Third party government vendor provides no notice to integrator/user of product changes/support.

JMV002. Stability/Robustness. Many upgrades.

JMV003. Complexity/Features. Dependencies on installation of MetCast Client and Netscape. Dependent on MetCast Client installation for needed executable files. Dependent on Netscape version.

RISK ASSESSMENT CHART

Product Name/Version:

Transition 1.3 (Metcast Client 1.1.0.3)

Assessment Date: September 28, 1999

Assessed By: Lorraine Smith

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	M
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	M
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	M
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	M
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	M
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	M
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

RISK ASSESSMENT CHART

Product Name/Version:

Transition 1.3 (Netscape Communicator 4.6.1)

Assessment Date: September 28, 1999

Assessed By: Lorraine Smith

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	L
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	M
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	M
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	M
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	H
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

NETSCAPE001. Complexity/Features. We customize the install to prevent load of real player, which cannot be installed. There are other unnecessary features.

NOTE: Netscape version chosen to satisfy JMV version.

RISK ASSESSMENT CHART

Product Name/Version:

Transition 1.3 (SMOOS Remote/Server 3.0)

Assessment Date: September 28, 1999

Assessed By: Lorraine Smith

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	M
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	M
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	M
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	L
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	M
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	M
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	M
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	M
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	M
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	M
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	M
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

RISK ASSESSMENT CHART

Product Name/Version:

Vector Map Level 0 EURNASIA 3.0

Assessment Date: October 5, 1999

Assessed By: Kyle Cunningham

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	L
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	M
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	M
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

RISK ASSESSMENT CHART

Product Name/Version:

Vector Map Level 0 NOAMER 4.0

Assessment Date: October 5, 1999

Assessed By: Kyle Cunningham

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	L
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	M
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	M
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

RISK ASSESSMENT CHART

Product Name/Version:

Vector Map Level 0 SASAUS 3.0

Assessment Date: October 5, 1999

Assessed By: Kyle Cunningham

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	L
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	M
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	M
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

RISK ASSESSMENT CHART

Product Name/Version:

Vector Map Level 0 SOAMAFR 3.0

Assessment Date: October 5, 1999

Assessed By: Kyle Cunningham

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	L
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	M
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	M
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

RISK ASSESSMENT CHART

Product Name/Version:

Windows 95 4.00.95.c

Assessment Date: October 5, 1999

Assessed By: Donald T. Gates

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	L
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	L
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	H
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	H
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

WIN95001. Security. Win 95 O/S is not secure. May impact systems certification and accreditation.

WIN95002. Stability/Robustness. Significant upgrade (Win 95 to Win 2000). Apps will require recompile to Win 2000.

RISK ASSESSMENT CHART

Product Name/Version:

Windows NT Server and Workstation 4.0

Assessment Date: October 5, 1999

Assessed By: Donald T. Gates

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	L
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	M
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	H
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	H
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

WINNT001. Stability/Robustness. O/S has always had problems with stability and robustness. The current patch to the O/S (SP5) has a minor Y2K issue.

WINNT002. Security. The default installation leaves the system in an insecure state. System certification and accreditation issues.

RISK ASSESSMENT CHART

Product Name/Version:

Win EOTDA 1.3.3

Assessment Date: October 5, 1999

Assessed By: Donald T. Gates

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	M
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	L
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	L
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	L
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

RISK ASSESSMENT CHART

Product Name/Version:

WinZip32 7.0 SR1

Assessment Date: October 5, 1999

Assessed By: Kyle Cunningham

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	L
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	L
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	M
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	M
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

RISK ASSESSMENT CHART

Product Name/Version:

WsFTP 6.0

Assessment Date: October 5, 1999

Assessed By: Kyle Cunningham

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	L
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	L
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	M
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	H
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

WSFTP001. Stability/Robustness. Y2K display problem. Requires patch.

RISK ASSESSMENT CHART

Product Name/Version:

ZipTools NE5305 5.4

Assessment Date: October 5, 1999

Assessed By: Donald T. Gates

Risk Category	Risk Factor	Risk Cues			Rating
		Low	Medium	High	
Technology	Maturity/Stability	Widely accepted technology.	Competing technologies.	Emerging technology.	L
	Competition	Large number of competing products within the selected technology.	Limited number of competing products within the selected technology.	Small number of competing products or no competition within the selected technology.	M
Vendor	Maturity/Stability	Large company. Applies commercially accepted development practices.	Medium company. Applies a mix of commercially accepted and ad-hoc development practices.	Small/emerging company. Applies ad-hoc development practices.	L
	Technology Expertise	Maintains personnel base with expertise in the technology.	Access to personnel with technology expertise. Moving into an emerging technology.	Limited or no access to personnel with technology expertise.	L
	Responsiveness	Accepts/processes customer feedback. Provides advance notice of product changes.	Accepts/processes market feedback. Provides limited notice of product changes.	Does not accept/process customer feedback. Provides no notice of product changes.	L
	Technical Support	Maintains knowledgeable technical support staff. Maintains 24/7 help desk. Easy access to help desk. Easy access to patches.	Maintains semi-knowledgeable technical support staff. Restricted help desk availability. Limited avenues to access help desk. Limited access to patches.	Knowledgeable technical assistance staff not available. No help desk. No access to patches.	L
Product	Market Acceptance	Wide market acceptance. Large market share. Product drives the market.	Limited market acceptance. Medium market share.	Product not widely accepted by the market. Small market share.	L
	Stability/Robustness	Very few significant upgrades. No significant bugs or limited insignificant bugs.	Moderate number of product upgrades/patches. Tolerable bugs (non-critical).	Significant number of product upgrades/patches. Significant or intolerable bugs.	L
	Interfaces	Uses commercially accepted interfaces. Interface documentation is available.	Uses a mix of commercially accepted interfaces and nonstandard or proprietary interfaces. Limited interface documentation.	Uses nonstandard or proprietary interfaces. No interface documentation.	L
	Complexity/Features	Easy to use. Easy to install and configure. Few extraneous capabilities. No undesirable features.	Moderately easy to use. Moderately easy to install or configure. Some extraneous capabilities. May have an undesirable feature.	Hard to use. Difficult to install or configure. Large number of extraneous capabilities. Exhibits undesirable features.	L
	Security	No significant security issues. No insignificant security issues.	No significant security issues. A few insignificant security issues.	Significant security issues. Many insignificant security issues.	L
	Safety	No safety issues.	N/A	Safety issue.	L
	Documentation	Understandable, complete, and accurate documentation package.	Acceptable documentation package. Falls short in some areas.	Poor documentation package.	L
	Cost	Competitive product cost. Good warranty. Reasonable maintenance fees.	Inflated product cost. Poor warranty. Inflated maintenance fees.	Unreasonable product cost. No warranty. Unreasonable maintenance fees.	L

NOTES:

APPENDIX B
METMF(R) RISK INFORMATION SHEETS

ID: ARCPRESS001	RISK INFORMATION SHEET		Identified: 10 OCT 99
Rating: MED	**Statement:** Y2K. Vendor announces minor Y2K display problem that requires a patch to correct. If this patch is not issued, the system is not Y2K compliant.		
Probability: HIGH			
Impact: LOW			
Timeframe: IMMED			
Context	Origin: K. Cunningham	Assigned To: K. Cunningham	Update Date: 15 NOV 99

Vendor Web Page (7/29/99). The ArcPress banner option, -B{file} displays the year portion of the date incorrectly when in the year 2000 or beyond. ArcPress calculates the number of years since 1900 then prepends "19" to that amount (e.g., in the year 2000, ArcPress banner date will read "19100"). A patch is available that fixes this display problem. The METMF(R) has been certified as Y2K compliant. Without the ArcPress patch, the METMF(R) is technically not Y2K compliant. This risk is deemed high priority due to political/programmatic reasons.

Mitigation Strategy

1. Assess impact of the banner option, -B{file}.
2. Obtain upgrade as soon as possible and test in the MSL.
3. Add upgrade to the METMF(R) baseline and release to the fleet prior to end of Dec (or iaw Y2K war-room policy) OR since this problem does not impact the system, incorporate the patch into the next planned baseline upgrade (MAR 00).
4. Monitor EEC to obtain status on other possible Y2K problems.

Contingency Plan

1. Release msg to the fleet identifying the banner option as a known problem with no impact to the User OR no action (depends on strategy 3 above).

Trigger: Patch not released by 10 December 1999.

Status

1. Discuss mitigation strategy/contingency plan w/SPONSOR. Approved. 12OCT99
2. Conducted banner option assessment. No operational impact. Very minor display problem that will not create confusion. Effort to release patch prior to Jan 00 outweighs benefits. Plan to evaluate for next baseline update. 15NOV99.
3. RAC Rating reduced to Medium. 15NOV99.

Approval	Closing Date	Closing Rationale
B. Hensley	MITIGATE	

ID: ARCVIEW001	RISK INFORMATION SHEET		Identified: 10 OCT 99
Rating: MED	Statement: Y2K. VENDOR announces minor Y2K display problem that requires a patch to correct. If this patch is not issued, the system is not Y2K compliant.		
Probability: HIGH			
Impact: LOW			
Timeframe: IMMED			
Context	Origin: K. Cunningham	Assigned To: K. Cunningham	Update Date: 15 NOV 99

Vendor Web Page (7/29/99). The ArcView License Manager diagnostic tool, FLEXlm's *lmutil* displays the incorrect date when in the year 2000 or beyond (e.g., for 3/1/2000, the *lmutil* tool will display: "lmutil – Copyright © 1989 – 1997 Globetrotter Software, Inc. FLEXlm diagnostics on Wed 3/1/100 13:36".
A patch is available that fixes this display problem (either FLEXlm version 6.0i and higher or ArcView Version 3.1). The METMF(R) has been certified as Y2K compliant. Without the ArcView upgrade or the FLEXlm patch, the METMF(R) is technically not Y2K compliant. This risk is deemed high priority due to political/programmatic reasons.

Mitigation Strategy

1. Assess impact of the lmutil function.
2. Obtain ArcPress upgrade as soon as possible and test in the MSL.
3. Add upgrade to the METMF(R) baseline and release to the fleet prior to end of Dec (or iaw Y2K war-room policy) OR since this problem does not impact the system, incorporate the patch into the next planned baseline upgrade (MAR 00).
4. Monitor EEC to obtain status on other possible Y2K problems.

Contingency Plan

1. Release msg to the fleet identifying the lmutil function as a known problem with no impact to the User.

Trigger: Patch not released by 10 December 1999.

Status

1. Discuss mitigation strategy/contingency plan w/SPONSOR. Approved. 12OCT99
2. Conducted lmutil function assessment. No operational impact. Very minor display problem that will not create confusion.
3. Effort to release patch prior to Jan 00 outweighs benefits. Plan to evaluate for next baseline update. 15NOV99.
4. RAC Rating reduced to Medium 15NOV99.

Approval	Closing Date	Closing Rationale
B. Hensley	MITIGATE	

ID: HPUX001	RISK INFORMATION SHEET	Identified: 10 OCT 99
Rating: HIGH Probability: HIGH Impact: HIGH Timeframe: FAR	**Statement:** HP may be phasing out HP-UX 10.20 in lieu of HP-UX 11.xx. May impact technical support. Migration to HP-UX 11.xx will affect all resident apps.	
Context	**Origin:** B. Hensley	**Assigned To:** J. Streker / **Update Date:** 12 OCT 99

NewsFlash: DISA recommends that the HP-UX COE baseline be updated to HP-UX 11.xx resulting in an HP-UX 11.xx DII COE 4.2 baseline (APR 00). HP will drop support for HP-UX 10.20 and will be reluctant to address customer issues (Y2K, security, error corrections, etc.). HP-UX will not run on HP 750/755 platforms. The METMF(R) runs HP-UX 10.20 on two HP J-210 TAC-4 platforms (MSS, MWS).

Mitigation Strategy

1. Contact vendors of software components that run on the MSS and the MWS and discuss their plans to migrate to HP-UX 11.xx.
2. Collect HP-UX 11.xx data. Perform qualification testing and risk assessment.
3. Obtain HP-UX 11.xx as soon as available and test in the MSL (functional and integration).
4. Monitor HP-UX 10.20 to obtain status on extant/new Y2K/Security/other problems that may not be addressed by the vendor.
5. Plan to incorporate HP-UX 11.xx in the AUG.99 or later baseline upgrade

Contingency Plan

1. None.

Trigger: None.

Status

1. Discuss mitigation strategy/contingency plan w/SPONSOR. Approved. 12OCT99
2. Establish HP-UX folder and perform continuous market survey to capture vendor/product data. 12OCT99

Approval	Closing Date	Closing Rationale
B. Hensley	MITIGATE	

ID: JMV001	RISK INFORMATION SHEET		Identified: 01 OCT 99
Priority: HIGH Probability: HIGH Impact: HIGH Timeframe: NEAR	**Statement:** GOVT Vendor plans to terminate OTH Gold data distribution and start GRIB data distribution. JMV 3.1.0.3 requires an upgrade to accept GRIB data.		
Context	**Origin:** Don Gates	**Assigned To:** K. Cunningham	**Update Date:** 17 NOV 99

GOVT Vendor plans to phase out OTH Gold support due to non-Y2K compliant servers and replace with GRIB data servers. Without patch (or upgrade), the METMF(R) will be unable to ingest JMV GRIB data with the new GRIB server. JMV upgrade will require CCB and Y2K War Room approval. Without approval, the fleet will not be able to ingest GRIB data.

Mitigation Strategy

1. Coordinate with GOVT Vendor to address OTH Gold data support requirements.
2. Download the fixed version of JMV 3.1.0.3 patch from "GOVT WEB PAGE".
3. Install the JMV 3.1.0.3 patch into MSL METMF(R) machines for testing and evaluation.
4. Add upgrade to the METMF(R) baseline and release to the fleet with next set of patches.

Contingency Plan

1. Release msg to the fleet identifying the termination of OTH Gold, operational impact, and plans to release JMV update for GRIB processing.

Trigger: OTH Gold support rqmnt not resolved and patch not released by 10 December 99.

Status

1. Discuss mitigation strategy/contingency plan w/SPONSOR. Approved 12 OCT99.
2. SPONSOR coord with GOVT Vendor => vendor will continue to support OTH Gold into FY00.
3. Incorporate Transition (JMV) upgrade as soon as available.

Approval	Closing Date	Closing Rationale
B. Hensley	MITIGATE	

ID: TERA001	RISK INFORMATION SHEET		Identified: 01 OCT 99
Priority: HIGH Probability: HIGH Impact: HIGH Timeframe: IMMED	**Statement:** TeraScan 3.0 requires an upgrade to restore lost functionality. Without the upgrade, users will not be able to process NOAA-15 data and will be unable to receive NOAA-14 TOVS data.		
Context	**Origin:** Don Gates	**Assigned To:** K. Cunningham	**Update Date:** 17 NOV 99

The vendor found Y2K issues w/TeraScan version 2.6 and released 3.0 as a Y2K compliant fix. Version 3.0 resulted in loss of many capabilities provided by version 2.6. The vendor is working on patch.

Mitigation Strategy

1. Install the new patches into the MSL for testing and evaluation.
2. Install the patches at a functional site (i.e. Camp Pendleton) for integration testing.
3. Add upgrade to the METMF(R) baseline and release to the fleet with next set of patches.

Contingency Plan

1. None

Trigger: None.

Status

1. Discuss mitigation strategy/contingency plan w/SPONSOR.
2. Obtain TeraScan patches from Vendor and conducted functional testing in the MSL and integration testing at MWSS 372 Camp Pendleton.
3. Patch considered unstable and unacceptable. Test results forwarded to vendor for action. 19NOV99
4. Developed patch SPCR (recommending disapproval). Submitted to SPONSOR for CCB approval.

Approval	Closing Date	Closing Rationale
B. Hensley	MITIGATE	

ID: WINNT001	RISK INFORMATION SHEET		Identified: 01 OCT 99
Priority: HIGH Probability: HIGH Impact: MED Timeframe: NEAR	**Statement:** Windows NT 4.0 (SP5) post patches fixes a Year2000 date problem with BIOS date value and net user /time command. Without the patches the BIOS date value does not immediately update on January 1, 2000 and the net users /time command does not work in the year 2000.		
Context	**Origin:** Don Gates	**Assigned To:** K. Cunningham	**Update Date:** 17 NOV 99

The METMF(R) has been certified as Y2K compliant. Microsoft previously certified WinNT 4.0 (SP5) as Y2K compliant but now requires Y2K patches. METMF(R) uses WinNT 4.0 (SP5). A software upgrade to the current METMF(R) software baseline requires approval by the SPONSOR CCB and the Y2K war-room. Without patch (or upgrade), the METMF(R) is no longer Y2K compliant.

Mitigation Strategy

1. Since this issue applies fleet-wide, seek (via SPONSOR) the Y2K war-room policy.
2. Assess Y2K impact.
3. Download the fixed version of WinNT 4.0 Post SP5 patches from http://support.microsoft.com/support/kb/articles/q216/9/13.asp (BIOS date value) and from http://support.microsoft.com/support/kb/articles/q240/1/95.asp (/time command)
4. Install the WinNT 4.0 SP5 post patches into MSL METMF(R) machines for testing and evaluation.
5. Develop SPCR to add upgrade to the METMF(R) baseline and release to the fleet with next set of patches.

Contingency Plan

1. Release msg to the fleet that identifies the Y2K problems.

Trigger: Y2K patch not released by 10 Dec 99

Status

1. Discuss mitigation strategy/contingency plan w/SPONSOR. Approved. 12OCT99
2. Unable to reproduce BIOS Date Y2K problem during MSL functional test and MWSS 372 integration test. Reproduced NET USER/Time command during functional and integration test and verified that patch solves problem. 17NOV99.
3. RAC Rating reduced to Medium. 17NOV99.
4. Developed patch SPCR. Submitted to SPONSOR for CCB approval and Y2K War Room disposition.

Approval	Closing Date	Closing Rationale
B. Hensley	MITIGATE	

ID: WSFTP001	RISK INFORMATION SHEET		Identified: 01 OCT 99
Priority: MED Probability: HIGH Impact: MED Timeframe: NEAR	**Statement:** WSFTP Pro requires a patch (or upgrade) to resolve a possible Y2K date display problem. Without the patch (or upgrade), the METMF(R) is no longer Y2K compliant.		
Context	**Origin:** Don Gates	**Assigned To:** K. Cunningham	**Update Date:** 17 NOV 99

The METMF(R) has been certified as Y2K compliant. The VENDOR previously certified WSFTP 6.0 as Y2K compliant but now requires installation of a patch (or upgrade) to resolve a new Y2K problem. METMF(R) uses WSFTP 6.0. In addition to the Y2K fix, the patch includes host type changes for IBM VM systems, corrected file date parsing, and drag and drop multiple transfers on Win2K RC1&2 for both Classic and Explorer interfaces. A software upgrade to the current METMF(R) software baseline requires approval by the SPONSOR CCB and the Y2K war-room.

Mitigation Strategy

1. Assess Y2K impact.
2. Download the fixed version of WSFTP Pro 6.04 from VENDOR WEB PAGE
3. Develop SPCR to add the patch to the baseline (includes test and evaluation)

Contingency Plan

1. Release a message to all METMF(R) users warning of WSFTP Pro Y2K display error and provide workaround.

Trigger: Patch not released by 10 Dec 99

Status

1. Discuss mitigation strategy/contingency plan w/SPONSOR. Approved. 12OCT99
2. Unable to reproduce Y2K problem (may only affect IBM VM computers) during MSL functional test and MWSS 372 integration test.
3. Developed patch SPCR. Submitted to SPONSOR for CCB approval and Y2K War Room disposition.

Approval	Closing Date	Closing Rationale
B. Hensley	MITIGATE	

LIST OF REFERENCES

[1] Carney, David J., Obendorf, Patricia A., "The Commandments of COTS: Still in Search of the Promised Land," Software Engineering Institute, Carnegie Mellon University, *Crosstalk*, May 1997.

[2] Brooks, Frederick P., *The Mythical Man-Month: Essays on Software Engineering*, Addison-Wesley, 1995.

[3] Fox, G., Lantner, K., Marcom, S., "A Software Development Process for COTS-Based Information System Infrastructure Part II: Lessons Learned," Software Engineering Institute, Carnegie Mellon University, *Crosstalk*, April 1998.

[4] Vigder, M. R., Gentleman, W. M., Dean, J., "COTS Software Integration: State of the Art," National Research Council of Canada, *NRC Report Number 39198*, January 1996.

[5] Tracz, W. Ph.D., "Architecture Issues, other Lessons Learned in Component-Based Software Development," Software Engineering Institute, Carnegie Mellon University, *Crosstalk*, January 2000.

[6] Jarzombek, J. LtCol., "The Double-Edged COTS IT Sword," Software Engineering Institute, Carnegie Mellon University, *Crosstalk*, April 1998.

[7] Brownsword, L., Carney, D., Oberndorf, T., "The Opportunities and Complexities of Applying Commercial-Off-the-Shelf Components," Software Engineering Institute, Carnegie Mellon University, *Crosstalk*, April 1998.

[8] Fairley, R., *Software Engineering Concepts*, McGraw-Hill, Inc., 1985.

[9] United States, General Services Administration, Federal Acquisition Regulation

[10] DoD Directive 5000.1, "Defense Acquisition," 15 March 1996.

[11] DoD Regulation 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAP) and Major Automated Information System (MAIS) Acquisition Programs,"March 1996.

[12] Oberndorf, P., Carney, D., "A Summary of DoD COTS-Related Policies," SEI Monographs on the Use of Commercial Software in Government Systems, Software Engineering Institute, Carnegie Mellon University, September 1998. http://www.sei.cmu.edu/cbs/papers/monographs/dod-cots-policies/dod-cots-policies.html

[13] Wallnau, K. C., "A Basis for COTS Software Evaluation: Foundations for the Design of COTS-Intensive Systems," SEI Monographs, Software Engineering Institute, Carnegie Mellon University.

[14] Fox, G., Lantner, K., Marcom, S., "A Software Development Process for COTS-Based Information System Infrastructure: Part I," Software Engineering Institute, Carnegie Mellon University, *Crosstalk*, March 1998.

[15] Military Standard, "Defense System Software Development," DoD-Std-2167A, 29 February 1988.

[16] Wells, J., "Overview of IEEE/EIA 12207: Standard for Information Technology," Software Engineering Process Office, Space and Naval Warfare Systems Center San Diego, 30 July 1998.

[17] Software Engineering Institute, *Proceedings of the SEI/MCC Symposium on the Use of COTS in Systems Integration*, Special Report CMU/SEI-95-SR-007, June 1995.

[18] Carney, D., "COTS Product Evaluation and System Design," SEI Interactive, COTS Spot, March 1999. http://interacive.sei.cmu.edu/columns/cots_spot/1999/march/cots.mar99.html

[19] Dean, C. D., Vigder, M. R., "System Implementation Using Commercial Off-The-Shelf (COTS) Software," National Research Council of Canada, *NRC Report Number 40173*, 1997.

[20] Gee, K., "An Architectural Framework for Integrating COTS/GOTS/Legacy Systems," Thesis, Naval Postgraduate School, Pending.

[21] Tran, T., Allen, J., "Interoperability of COTS Software Components with Legacy Systems in a Distributed Computing Environment," Thesis, Naval Postgraduate School, Pending.

[22] Osmundson, J., "Class Notes from Naval Postgraduate School Course IS4300, Software Project Management," 1998.

[23] Van Scoy, R. L., "Software Development Risk: Opportunity, Not Problem," SEI Technical Report CMU/SEI-92-TR-30, ESC-TR-92-030, September 1992.

[24] West-Brown, M., Hernan, S. V., "What Messages Are You Sending to Vendors?," SEI Interactive, Security Matters, Vol. 1., Issue 3, December 1998. http://interactive.sei.cmu.edu/columns/security_matters/1998/december/security.dec98.html

[25] Dorofee, A. J., Walker, J. A., Williams R. C., "Risk Management in Practice," Software Engineering Institute, Carnegie Mellon University, *Crosstalk*, April 1997. http://www.stsc.hill.af.mil/crosstalk/1997/apr/management.asp

[26] Chief of Naval Operations Letter, Ref. CNO 3140 Serial 961, 64570953, 29 October 1999.

[27] Version Description Document for the Meteorological Mobile Facility (Replacement) (METMF(R)), Release 1.3, Space and Naval Warfare Systems Center, San Diego, August 1998.

[28] Military Handbook, "Configuration Management Guidance," Mil-Hdbk-61, 30 September 1997.

[29] Vidger, M. R., "An Architecture for COTS Based Software Systems," National Research Council of Canada, *NRC Report Number 41603*, 1 November 1998.

[30] Statz, J., Oxley, D., O'Toole, P., "Identifying and Managing Risks for Software Process Improvement," Software Engineering Institute, Carnegie Mellon University, *Crosstalk*, April 1997. http://www.stsc.hill.af.mil/crosstalk/1997/apr/identifying.asp

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   8725 John J. Kingman Rd., STE 0944
   Ft. Belvoir, Virginia 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Road
   Monterey, California 93943-5101

3. Chairman, Code CS 1
   Naval Postgraduate School
   Monterey, California 93943-5100

4. Dr. Luqi, CS/Lq 1
   Computer Science Department
   Naval Postgraduate School
   Monterey, California 93943-5100

5. Dr. Mantak Shing, Code CS/Sh 1
   Computer Science Department
   Naval Postgraduate School
   Monterey, California 93943-5100

6. Dr. John Osmundson, Code CC/Os 1
   C3 Academic Group
   Naval Postgraduate School
   Monterey, California 93943-5100

7. Barry J. Hensley 2
   11578 Windcrest Lane Apt #1826
   San Diego, California 92128